7TH EDITION

ROBERT
MOELLER

Brink's MODERN INTERNAL AUDITING

A Common Body of Knowledge

Brink's Modern Internal Auditing

Brink's Modern Internal Auditing

A Common Body of Knowledge

Seventh Edition

ROBERT R. MOELLER

WILEY
John Wiley & Sons, Inc.

Copyright © 2009 John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400, fax 978-646-8600, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, 201-748-6011, fax 201-748-6008, or online at http://www.wiley.com/go/permissions.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services, or technical support, please contact our Customer Care Department within the United States at 800-762-2974, outside the United States at 317-572-3993 or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

For more information about Wiley products, visit our Web site at http://www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Moeller, Robert R.
Brink's modern internal auditing : a common body of knowledge / Robert Moeller. – 7th ed.
p. cm.
Includes index.
ISBN 978-0-470-29303-4 (cloth: alk. paper) 1. Auditing, Internal. I. Title.
HF5668.25.B74 2009
657′.458–dc22

2008048335

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Contents

Preface xix

About the Author xxv

PART ONE FOUNDATIONS OF MODERN INTERNAL AUDITING 1

CHAPTER 1 Foundations of Internal Auditing 3

1.1 Internal Auditing History and Background 5
1.2 Organization of This Book 8
Note 10

CHAPTER 2 Internal Audit's Common Body of Knowledge 11

2.1 What Is a CBOK?: Experiences from Other Professions 12
2.2 Institute of Internal Auditor's Research Foundation CBOK 13
2.3 What Does an Internal Auditor Need to Know? 18
2.4 Modern Internal Auditing's CBOK Going Forward 19
Notes 19

PART TWO IMPORTANCE OF INTERNAL CONTROLS 21

CHAPTER 3 Internal Control Framework: The COSO Standard 23

3.1 Importance of Effective Internal Controls 23
3.2 Internal Controls Standards: Background 25
(a) Internal Control Definitions: Foreign Corrupt Practices Act of 1977 26
(b) FCPA Aftermath: What Happened? 28
3.3 Events Leading to the Treadway Commission 28
(a) Earlier AICPA Standards: SAS No. 55 30
(b) Treadway Committee Report 30
3.4 COSO Internal Control Framework 31
(a) Control Environment 33
(b) Risk Assessment 39
(c) Control Activities 41
(d) Communications and Information 43
(e) Monitoring 46

3.5 Other Dimensions of the COSO Internal Controls Framework 50
3.6 Internal Audit CBOK Needs 51
Notes 51

CHAPTER 4 Sarbanes-Oxley and Beyond 53

4.1 Key Sarbanes-Oxley Act Elements 54
(a) Title I: Public Company Accounting Oversight Board 55
(b) Title II: Auditor Independence 60
(c) SOx Title III: Corporate Responsibility 62
(d) Title IV: Enhanced Financial Disclosures 68
(e) Title V: Analyst Conflicts of Interest 72
(f) Titles VI through X: Fraud Accountability and White-Collar Crime 72
(g) Title XI: Corporate Fraud Accountability 74
4.2 Performing Section 404 Reviews under AS 5 75
(a) Section 404 Internal Controls Assessments Today 75
(b) Launching the Section 404 Compliance Review 76
4.3 AS 5 Rules and Internal Audit 84
4.4 Impact of the Sarbanes-Oxley Act 87
Notes 87

CHAPTER 5 Another Internal Controls Framework: CobiT 89

5.1 Introduction to CobiT 90
5.2 CobiT Framework 92
(a) CobiT Cube Components: IT Resources 94
(b) CobiT Cube Components 94
5.3 Using CobiT to Assess Internal Controls 96
(a) Planning and Enterprise 98
(b) Acquisition and Implementation 100
(c) Delivery and Support 102
(d) Monitoring and Evaluation 103
5.4 Using CobiT in a SOx Environment 107
5.5 CobiT Assurance Framework Guidance 110
5.6 CobiT in Perspective 111
Notes 111

CHAPTER 6 Risk Management: COSO ERM 113

6.1 Risk Management Fundamentals 114
(a) Risk Identification 115
(b) Key Risk Assessments 118
(c) Quantitative Risk Analysis 121
6.2 COSO ERM: Enterprise Risk Management 124
6.3 COSO ERM Key Elements 126
(a) Internal Environment Component 127
(b) Objective Setting 129
(c) Event Identification 132

(d) Risk Assessment 134
(e) Risk Response 136
(f) Control Activities 138
(g) Information and Communication 140
(h) Monitoring 141
6.4 Other Dimensions of COSO ERM: Enterprise Risk Objectives 142
(a) Operations Risk Management Objectives 142
(b) Reporting Risk Management Objectives 143
(c) Legal and Regulatory Compliance Risk Objectives 143
6.5 Entity-Level Risks 145
(a) Risks Encompassing the Entire Organization 145
(b) Business Unit–Level Risks 145
6.6 Putting It All Together 146
6.7 Auditing Risk and COSO ERM Processes 146
6.8 Risk Management and COSO ERM in Perspective 147
Notes 149

PART THREE PLANNING AND PERFORMING INTERNAL AUDITS 151

CHAPTER 7 Performing Effective Internal Audits 153

7.1 Organizing and Planning Internal Audits 154
7.2 Internal Audit Preparatory Activities 155
(a) Determine the Audit Objectives 157
(b) Audit Scheduling and Time Estimates 158
(c) Preliminary Surveys 159
7.3 Starting the Internal Audit 160
(a) Internal Audit Field Survey 163
(b) Documenting the Internal Audit Field Survey 164
(c) Field Survey Auditor Conclusions 165
7.4 Developing and Preparing Audit Programs 166
(a) Audit Program Formats and Their Preparation 167
(b) Types of Audit Evidence 171
7.5 Performing the Internal Audit 172
(a) Internal Audit Fieldwork Initial Procedures 173
(b) Audit Fieldwork Technical Assistance 175
(c) Audit Management Fieldwork Monitoring 175
(d) Potential Audit Findings 176
(e) Audit Program and Schedule Modifications 178
(f) Reporting Preliminary Audit Findings to Management 178
7.6 Wrapping Up the Field Engagement Internal Audit 179
7.7 Performing an Individual Internal Audit 180

CHAPTER 8 Standards for the Professional Practice of Internal Auditing 183

8.1 Internal Auditing Professional Practice Standards 184
(a) Background of the IIA Standards 184

(b) IIA's Current Standards: What Has Changed 186
(c) 2009 New Internal Audit Standards 187
8.2 Content of the IIA Standards 187
(a) Internal Audit Attribute Standards 188
(b) Internal Audit Performance Standards 191
8.3 Codes of Ethics: The IIA and ISACA 196
Notes 198

CHAPTER 9 Testing, Assessing, and Evaluating Audit Evidence 199

9.1 Gathering Appropriate Audit Evidence 199
9.2 Audit Assessment and Evaluation Techniques 200
9.3 Internal Audit Judgmental Sampling 202
9.4 Statistical Sampling: An Introduction 204
(a) Statistical Sampling Concepts 205
(b) Developing a Statistical Sampling Plan 210
(c) Audit Sampling Approaches 214
9.5 Monetary Unit Sampling 225
(a) Selecting the Monetary Unit Sample: An Example 225
(b) Performing the Monetary Unit Sampling Test 227
(c) Evaluating Monetary Unit Sample Results 228
(d) Monetary Unit Sampling Advantages and Limitations 228
9.6 Variables and Stratified Variables Sampling 229
9.7 Other Audit Sampling Techniques 232
(a) Multistage Sampling 232
(b) Replicated Sampling 232
(c) Bayesian Sampling 233
9.8 Making Efficient and Effective Use of Audit Sampling 233
Notes 236

CHAPTER 10 Audit Programs and Establishing the Audit Universe 237

10.1 Defining the Scope and Objectives of the Internal Audit Universe 238
10.2 Assessing Internal Audit Capabilities and Objectives 242
10.3 Audit Universe Time and Resource Limitations 244
10.4 "Selling" the Audit Universe to the Audit Committee and Management 245
10.5 Assembling Audit Programs: Audit Universe Key Components 247
(a) Audit Program Formats and Their Preparation 248
(b) Types of Program Audit Evidence 251
10.6 Audit Universe and Program Maintenance 252

CHAPTER 11 Control Self-Assessments and Benchmarking 253

11.1 Importance of Control Self-Assessments 253
11.2 CSA Model 254

11.3 Launching the CSA Process 255
(a) Performing the Facilitated CSA Review 257
(b) Performing the Questionnaire-Based CSA Review 259
(c) Performing the Management-Produced Analysis CSA Review 261
11.4 Evaluating CSA Results 261
11.5 Benchmarking and Internal Audit 262
(a) Implementing Benchmarking to Improve Processes 263
(b) Benchmarking and the IIA's GAIN Initiative 265
11.6 Better Understanding Internal Audit Activities 269
Notes 269

PART FOUR ORGANIZING AND MANAGING INTERNAL AUDITOR ACTIVITIES 271

CHAPTER 12 Internal Audit Charters and Building the Internal Audit Function 273

12.1 Establishing an Internal Audit Function 274
12.2 Audit Charter: Audit Committee and Management Authority 274
12.3 Building the Internal Audit Staff 275
(a) Role of the CAE 277
(b) Internal Audit Management Responsibilities 278
(c) Internal Audit Staff Responsibilities 278
(d) Information Systems Audit Specialists 281
(e) Other Internal Auditor Specialists 281
12.4 Internal Audit Department Organization Approaches 283
(a) Centralized versus Decentralized Internal Audit Organization Structures 283
(b) Organizing the Internal Audit Function 285
12.5 Internal Audit Policies and Procedures 290
12.6 Professional Development: Building a Strong Internal Audit Function 292
Note 292

CHAPTER 13 Internal Audit Key Competencies 293

13.1 Importance of Internal Audit Key Competencies 293
13.2 Internal Auditor Interview Skills 294
13.3 Analytical Skills 296
13.4 Testing and Analysis Skills 296
13.5 Internal Auditor Documentation Skills 298
13.6 Recommending Results and Corrective Actions 301
13.7 Internal Auditor Communication Skills 301
13.8 Internal Auditor Negotiation Skills 302

13.9 Internal Auditor Commitment to Learning 304
13.10 Importance of Internal Auditor Core Competencies 304

CHAPTER 14 Understanding Project Management 305

14.1 Project Management Processes 305
(a) Project Management Book of Knowledge 306
(b) Developing a Project Management Plan 310
14.2 *PMBOK* Program and Portfolio Management 311
14.3 Organizational Process Maturity Model 315
14.4 Using Project Management for Effective Internal Audit Plans 318
14.5 Project Management Best Practices and Internal Audit 318
Notes 319

CHAPTER 15 Planning and Performing Internal Audits 321

15.1 Understanding the Environment: Launching an Internal Audit 321
15.2 Documenting and Understanding the Internal Controls Environment 323
15.3 Performing Appropriate Internal Audit Procedures 325
15.4 Wrapping Up the Internal Audit 326
15.5 Performing Internal Audits 328

CHAPTER 16 Documenting Results through Process Modeling and Workpapers 329

16.1 Internal Audit Documentation Requirements 330
16.2 Process Modeling for Internal Auditors 331
(a) Understanding the Process Modeling Hierarchy 332
(b) Describing and Documenting Key Processes 332
(c) Process Modeling and the Internal Auditor 334
16.3 Internal Audit Workpapers 335
(a) Workpaper Standards 338
(b) Workpaper Formats 339
(c) Workpaper Document Organization 340
(d) Workpaper Preparation Techniques 344
(e) Workpaper Review Processes 347
16.4 Internal Audit Document Records Management 347
16.5 Importance of Internal Audit Documentation 349
Note 350

CHAPTER 17 Reporting Internal Audit Results 351

17.1 Purposes and Types of Internal Audit Reports 351
17.2 Published Audit Reports 353
(a) Approaches to Published Audit Reports 354
(b) Elements of an Audit Report Finding 358

(c) Balanced Audit Report Presentation Guidelines 362
(d) Alternative Audit Report Formats 363
17.3 Internal Audit Reporting Cycle 366
(a) Draft Audit Reports 368
(b) Audit Reports: Follow-Up and Summary 371
(c) Audit Report and Workpaper Retention 372
17.4 Effective Internal Audit Communications Opportunities 373
17.5 Audit Reports and Understanding the People in Internal Auditing 376

PART FIVE IMPACT OF INFORMATION TECHNOLOGY ON INTERNAL AUDITING 379

CHAPTER 18 IT General Controls and ITIL Best Practices 381

18.1 Importance of IT General Controls 382
18.2 Client-Server and Smaller Systems' General IT Controls 383
(a) General Controls for Small Business Systems 384
(b) Smaller Systems' IT Operations Internal Controls 388
(c) Auditing IT General Controls for Smaller IT Systems 390
18.3 Components and Controls of Mainframe and Legacy Systems 394
(a) Characteristics of Larger IT Systems 394
(b) Classic Mainframe or Legacy Computer Systems 396
(c) Operating Systems Software 397
18.4 Legacy System General Controls Reviews 399
18.5 ITIL Service Support and Delivery Infrastructure Best Practices 405
(a) ITIL Service Support Incident Management 407
(b) Service Support Problem Management 409
18.6 Service Delivery Best Practices 414
(a) Service Delivery Service-Level Management 415
(b) Service Delivery Financial Management for IT Services 418
(c) Service Delivery Capacity Management 419
(d) Service Delivery Availability Management 421
(e) Service Delivery Continuity Management 422
18.7 Auditing IT Infrastructure Management 422
18.8 Internal Auditor CBOK Needs for IT General Controls 423
Notes 424

CHAPTER 19 Reviewing and Assessing IT Application Controls 425

19.1 IT Application Control Components 426
(a) Application Input Components 427
(b) Application Programs 429
(c) IT Application Output Components 434

19.2 Selecting Applications for Internal Audit Reviews 436
19.3 Preliminary Steps to Performing Applications Controls Reviews 437
(a) Conducting an Application Walk-Through 439
(b) Developing Application Control Objectives 442
19.4 Completing the IT Application's Controls Audit 443
(a) Clarifying and Testing Audit Internal Control Objectives 444
(b) Completing the Application Controls Review 448
19.5 Application Review Example: Client-Server Budgeting System 448
(a) Reviewing Capital Budgeting System Documentation 449
(b) Identifying Capital Budgeting Application Key Controls 450
(c) Performing Application Tests of Compliance 451
19.6 Auditing Applications under Development 451
(a) Objectives and Obstacles of Preimplementation Auditing 452
(b) Preimplementation Review Objectives 453
(c) Preimplementation Review Problems 454
(d) Preimplementation Review Procedures 455
19.7 Importance of Reviewing IT Application Controls 459
Notes 459

CHAPTER 20 Cybersecurity and Privacy Controls 461

20.1 IT Network Security Fundamentals 462
(a) Security of Data 463
(b) Importance of IT Passwords 464
(c) Viruses and Malicious Program Code 465
(d) Phishing and Other Identity Threats 467
(e) IT System Firewalls 468
(f) Other Computer Security Issues 469
20.2 IT Systems Privacy Concerns 469
(a) Data Profiling Privacy Issues 469
(b) Online Privacy and E-Commerce Issues 470
(c) Radio Frequency Identification 470
(d) Absence of U.S. Federal Privacy Protection Laws 471
20.3 Auditing IT Security and Privacy 472
20.4 Security and Privacy in the Internal Audit Department 474
(a) Security and Control for Auditor Computers 474
(b) Workpaper Security 475
(c) Audit Reports and Privacy 477
(d) Internal Audit Security and Privacy Standards and Training 477
20.5 PCI-DSS Fundamentals 477
20.6 Internal Audit's Privacy and Cybersecurity Roles 479
Notes 479

CHAPTER 21 Computer-Assisted Audit Tools and Techniques 481

21.1 Understanding Computer-Assisted Audit Tools and Techniques 482
21.2 Determining the Need for CAATTs 484
21.3 CAATT Software Tools 487
(a) Types of CAATTs: Generalized Audit Software 488
(b) Report Generators Languages 489
(c) Desktop and Laptop CAATTs 491
(d) Test Data or Test Deck Approaches 492
(e) Specialized Audit Test and Analysis Software 496
(f) Embedded Audit Procedures 496
21.4 Selecting Appropriate CAATT Processes 501
21.5 Steps to Building Effective CAATTs 501
21.6 Using CAATTs for Audit Evidence Gathering 503
Notes 504

CHAPTER 22 Business Continuity Planning and IT Disaster Recovery 505

22.1 IT Disaster and Business Continuity Planning Today 506
22.2 Auditing Business Continuity Planning Processes 508
(a) Internal Auditor Centralized Data Center BCP Reviews 508
(b) Client-Server Continuity Planning Internal Audit Procedures 513
(c) Continuity Planning for Desktop and Laptop Applications 513
22.3 Building the IT Business Continuity Plan 515
(a) Risks, Business Impact Analysis, and the Impact of Potential Emergencies 517
(b) Preparing for Possible Contingencies 519
(c) Disaster Recovery: Handling the Emergency 522
(d) Business Continuity Plan Enterprise Training 522
22.4 Business Continuity Planning and Service-Level Agreements 523
22.5 Newer Business Continuity Plan Technologies: Data Mirroring Techniques 524
22.6 Auditing Business Continuity Plans 526
22.7 Business Continuity Planning Going Forward 526
Notes 527

PART SIX INTERNAL AUDIT AND ENTERPRISE GOVERNANCE 529

CHAPTER 23 Board Audit Committee Communications 531

23.1 Role of the Audit Committee 532
23.2 Audit Committee Organization and Charters 533
23.3 Audit Committee's Financial Expert and Internal Audit 536

23.4 Audit Committee Responsibilities for Internal Audit 539
(a) Appointment of the Chief Audit Executive 541
(b) Approval of Internal Audit Charter 542
(c) Approval of Internal Audit Plans and Budgets 543
(d) Audit Committee Review and Action on Significant Audit Findings 545
23.5 Audit Committee and Its External Auditors 546
23.6 Whistleblower Programs and Codes of Conduct 546
23.7 Other Audit Committee Roles 547

CHAPTER 24 Ethics and Whistleblower Programs 549

24.1 Enterprise Ethics, Compliance, and Governance 550
(a) Ethics First Steps: Developing a Mission Statement 551
(b) Understanding the Ethics Risk Environment 553
(c) Summarizing Ethics Survey Results: Do We Have a Problem? 556
24.2 Enterprise Codes of Conduct 556
(a) Code of Conduct Contents: What Should Be the Code's Message? 557
(b) Communications to Stakeholders and Assuring Compliance 559
(c) Code Violations and Corrective Actions 560
(d) Keeping the Code of Conduct Current 561
24.3 Whistleblower and Hotline Functions 562
(a) Federal Whistleblower Rules 563
(b) SOx Whistleblower Rules and Internal Audit 564
(c) Launching an Enterprise Help or Hotline Function 565
24.4 Auditing the Enterprise's Ethics Functions 567
24.5 Improving Corporate Governance Practices 569
Notes 569

CHAPTER 25 Fraud Detection and Prevention 571

25.1 Understanding and Recognizing Fraud 572
25.2 Red Flags: Fraud Detection Signs for Internal Auditors 572
25.3 Public Accounting's Role in Fraud Detection 577
25.4 IIA Standards for Detecting and Investigating Fraud 580
25.5 Fraud Investigations for Internal Auditors 582
25.6 Information Technology Fraud Prevention Processes 583
25.7 Fraud Detection and the Internal Auditor 585
Notes 585

CHAPTER 26 HIPAA, GLBA, and Other Compliance Requirements 587

26.1 HIPAA: Healthcare and Much More 588
(a) HIPAA Patient Record Privacy Rules 589
(b) Cryptography, PKI, and HIPAA Security Requirements 591

(c) HIPAA Security Administrative Procedures 593
(d) Technical Security Services and Mechanisms 594
(e) Going Forward: HIPAA and E-Commerce 595
26.2 Gramm-Leach-Bliley Act Internal Audit Rules 595
(a) GLBA Financial Privacy Rules 596
(b) GLBA Safeguards Rule 598
(c) GLBA Pretexting Provisions 599
26.3 Other Personal Privacy and Security Legislative Requirements 600

PART SEVEN THE PROFESSIONAL INTERNAL AUDITOR 603

CHAPTER 27 Professional Certifications: CIA, CISA, and More 605

27.1 Certified Internal Auditor Responsibilities and Requirements 606
(a) The CIA Examination 607
(b) Maintaining Your CIA Certification 615
27.2 Beyond the CIA: Other IIA Certifications 615
(a) CCSA® Requirements 616
(b) CGAP® Requirements 616
(c) CFSA® Requirements 619
(d) Importance of the CIA Specialty Certification Examinations 619
27.3 Certified Information Systems Auditor (CISA) Requirements 619
27.4 Certified Information Security Manager® Certification 622
27.5 Certified Fraud Examiner 623
27.6 CISSP Information Systems Security Professional Certification 625
27.7 ASQ Internal Audit Certifications 625
27.8 Other Internal Auditor Certifications 626

CHAPTER 28 Internal Auditors as Enterprise Consultants 629

28.1 Standards for Internal Audit as an Enterprise Consultant 630
28.2 Launching an Internal Audit Internal Consulting Capability 631
28.3 Ensuring an Audit and Consulting Separation of Duties 633
28.4 Consulting Best Practices 635
(a) First Steps: Launching a Consulting Assignment 636
(b) Consulting Engagement Letters 637
(c) Consulting Process: Defining "As Is" and "To Be" Objectives 638
(d) Implementing Consulting Recommendations 640
(e) Documenting and Completing the Consulting Engagement 640
28.5 Expanded Internal Audit Services to Management 640
Note 641

CHAPTER 29 Continuous Assurance Auditing and XBRL 643

29.1 Implementing Continuous Assurance Auditing 644
(a) What Is a CAA Monitoring Process? 645
(b) Resources for Implementing CAA 648
29.2 Benefits of CAA 651
29.3 XBRL: Internet-Based Extensible Business Reporting Language 651
(a) XBRL Defined 652
(b) Implementing XBRL 652
29.4 Data Warehouses, Data Mining, and OLAP 655
(a) Importance of Storage Tools 655
(b) Data Warehouses and Data Mining 656
(c) Online Analytical Processing 658
29.5 Newer Technologies, the Continuous Close, and Internal Audit 659
Notes 660

PART EIGHT INTERNATIONAL AUDITING PROFESSIONAL CONVERGENCE CBOK REQUIREMENTS 661

CHAPTER 30 ISO 27001, ISO 9000, and Other International Standards 663

30.1 Importance of ISO Standards in Today's Global World 664
30.2 ISO Standards Overview 666
(a) ISO 9001 Quality Management Systems and Sarbanes-Oxley 667
(b) IT Security Standards: ISO 17799 and 27001 672
(c) IT Security Technique Requirements: ISO 27001 674
(d) Service Quality Management: ISO 20000 675
30.3 ISO 19011 Quality Management Systems Auditing 676
30.4 ISO Standards and Internal Auditors 678
Notes 678

CHAPTER 31 Quality Assurance Auditing and ASQ Standards 679

31.1 Duties and Responsibilities of Quality Auditors 680
31.2 Role of the Quality Auditor 681
31.3 Performing ASQ Quality Audits 685
31.4 Quality Auditors and the IIA Internal Auditor 687
31.5 Quality Assurance Reviews of the Internal Audit Function 688
(a) Benefits of an Internal Audit Quality-Assurance Review 689
(b) Elements of an Internal Audit Quality-Assurance Review 690
(c) Who Performs the Quality-Assurance Review? 692
31.6 Launching the Internal Audit Quality-Assurance Review 694
(a) Quality-Assurance Review Approaches 695

(b) Example Quality-Assurance Review of an Internal Audit Function 696
(c) Reporting the Results of an Internal Audit Quality-Assurance Review 702
31.7 Future Directions for Quality-Assurance Auditing 704
Notes 705

CHAPTER 32 Six Sigma and Lean Techniques 707

32.1 Six Sigma Background and Concepts 708
32.2 Implementing Six Sigma 709
(a) Six Sigma Leadership Roles and Responsibilities 711
(b) Launching the Six Sigma Project 714
32.3 Lean Six Sigma 716
32.4 Auditing Six Sigma Processes 718
32.5 Six Sigma in Internal Audit Operations 719
Note 721

CHAPTER 33 International Internal Auditing and Accounting Standards 723

33.1 International Accounting and Auditing Standards: How Did We Get Here? 724
33.2 Financial Reporting Standards Convergence 725
33.3 IFRS: What Internal Auditors Need to Know 727
33.4 International Internal Auditing Standards 728
33.5 Next Steps in Internal Audit Standards 729

CHAPTER 34 CBOK for the Modern Internal Auditor 731

34.1 Part One: Foundations of Modern Internal Auditing 732
34.2 Part Two: Importance of Internal Controls 732
34.3 Part Three: Planning and Performing Internal Audits 733
34.4 Part Four: Organizing and Managing Internal Audit Activities 733
34.5 Part Five: Impact of Information Technology on Internal Auditing 734
34.6 Part Six: Internal Audit and Enterprise Governance 735
34.7 Part Seven: The Professional Internal Auditor 735
34.8 Part Eight: Internal Auditing Professional Convergence CBOK Requirements 736
34.9 A CBOK for Internal Auditors 736
Note 737

Index 739

Preface

This book is a complete guide to the process and profession of internal auditing—what professionals need to know to successfully perform individual internal audits and what an enterprise needs to know to launch an effective internal audit function. With a heritage that goes back to the first days of internal auditing after World War II when Victor Brink produced the first edition, the chapters that follow describe modern internal auditing today. Although often misused, the word *modern* in Brink's original title says a lot about this book's heritage and the practice of internal auditing today. The title *Modern Internal Auditing* was used in the first edition to describe an evolving new profession at a time when internal auditors were often little more than accounting clerks or clerical support staff for external auditors. Brink envisioned internal auditors as professionals performing much broader services to management.

Today's internal auditors must operate in an ever-changing environment. There are many areas in which internal auditors need an increased level of knowledge and understanding, but sorting through what is important and areas that are just nice to know represents a challenge. This edition describes areas in which internal auditors should have a strong understanding as well as other areas in which internal auditors need only some knowledge and understanding. Combining both of these areas, this edition defines a common body of knowledge (CBOK) for the profession of internal auditing.

The practice of internal auditing is important to enterprises today on a worldwide basis, and members of senior management, government regulators, and other professionals need to have a general understanding and set of expectations of the roles and capabilities of internal auditors. That is, just as internal auditors need a CBOK to better define their profession, the outside world needs to better understand the responsibilities of internal auditors and how they can serve management at all levels.

The chapters to come describe a CBOK for internal auditors—knowledge areas that should be important to all internal auditors, no matter their level of experience, their business area, or where they are working in the world. The CBOK topics presented are based on this author's long-term experiences in internal auditing as well as extensive professional activities and reading.

Going beyond the table of contents, the following are some of the CBOK elements found in each chapter:

Part One: Foundations of Modern Internal Auditing. The two introductory chapters highlight the growing importance of internal auditing in all aspects of business, government, and other activities as well as why a CBOK is important.

1. **Foundations of Internal Auditing.** This introduction talks about the origins of internal auditing. The information is not really key CBOK but important background knowledge and history for today's internal auditor.
2. **Internal Audit's Common Body of Knowledge.** Here we explain and expand the concept of a CBOK and why it is important to all internal auditors.

Part Two: Importance of Internal Controls. The review and assessment of internal controls are key internal audit activities. The four chapters in this part describe internal controls reviews in terms of the Sarbanes-Oxley Act (SOx) requirements and several internal control frameworks.

3. **Internal Control Framework: The COSO Standard.** This internal control framework has become the worldwide standard for assessing internal controls; every internal auditor needs to understand the Committee of Sponsoring Organizations (COSO) internal control framework model and how to use it in assessments of internal controls.
4. **Sarbanes-Oxley and Beyond.** SOx became the law in the United States in 2002 and has completely changed how we assess and measure internal accounting controls almost worldwide. The chapter discusses the current status of SOx, including the newly released AS 5 auditing standards, and those SOx elements that are particularly important to internal auditors.
5. **Another Internal Controls Framework: CobiT.** In our very IT-dependent world, internal auditors need a framework to help them to measure and assess internal controls as part of their review efforts. The *C*ontrol *ob*jectives for *i*nformation and related *T*echnology (CobiT) tool is important here, and all internal auditors should have a least a general understanding of this internal control framework that is recognized worldwide.
6. **Risk Management: COSO ERM.** Risk management is an important internal audit knowledge area, and internal auditors need to understand and make use of the COSO Enterprise Risk Model (COSO ERM) as part of their internal audit planning and assessment activities. The chapter describes this risk assessment framework and why it is important for internal auditors.

Part Three: Planning and Performing Internal Audits. The five chapters in this part discuss some important general concepts and elements of the practice of modern internal auditing, ranging from professional governing standards to assessing those areas in the enterprise that should be candidates for internal audits.

7. **Performing Effective Internal Audits.** This chapter contains a fundamental introduction on the overall practice of planning, performing, and completing an effective internal audit. It describes the steps necessary to perform a review as an internal auditor.
8. **Standards for the Professional Practice of Internal Auditing.** All internal auditors need to have an understanding of these standards issued by the Institute of Internal Auditors (IIA). The chapter provides an overview of the more important elements of the standards and where to search for more information.
9. **Testing, Assessing, and Evaluating Audit Evidence.** A major activity in the internal audit process is to examine some record or artifact of audit evidence

and then to decide if it meets established audit review criteria. This is a basic internal audit knowledge area that must follow internal auditing best practices.

10. **Audit Programs and Establishing the Audit Universe.** Many areas in any enterprise are potential candidates for internal audit reviews, but internal auditors have a need to pare the list down to what is generally known as an audit universe. The chapter provides some guidance developing an audit universe schedule as well as information on how to build audit programs: the guides or actions steps necessary to perform internal audits.
11. **Control Self-Assessments and Benchmarking.** The IIA has developed extensive criteria for internal auditors to look at what they are doing at a specific time and to assess that work. The chapter describes these processes.

Part Four: Organizing and Managing Internal Audit Activities. The six chapters in this part discuss the process of launching, performing, and completing internal audits.

12. **Internal Audit Charters and Building the Internal Audit Function.** Best practices here cover the whole area of building and managing an effective internal audit function. The chapter's theme is on how a new enterprise would launch and build its own internal audit function, including an audit charter authorizing document.
13. **Internal Audit Key Competencies.** Beyond such technical skills as understanding SOx key requirements and information technology (IT) general controls, internal auditors must possess some other core key competencies, such as interviewing and writing skills. The chapter focuses on some of these necessary skills for all levels of internal auditors.
14. **Understanding Project Management.** Whether building an audit schedule for an upcoming fiscal period or planning a specific audit engagement, internal auditors at all levels need to have an understanding of good project management techniques. This chapter discusses project management for internal auditors.
15. **Planning and Performing Internal Audits.** Unlike most of the other chapters, which discuss some of the more technical knowledge skills necessary for internal audits, this chapter outlines the steps necessary to perform a typical, internal controls assessment internal audit.
16. **Documenting Results through Process Modeling and Workpapers.** Internal auditors need efficient and cost-effective procedures to review and document overall business processes of all types. Many alternatives are available here. This chapter introduces some good internal audit–based approaches to understand various process and then to document that work through audit workpapers.
17. **Reporting Internal Audit Results.** Reporting the results of internal audit work and recommendations for corrective actions is a major internal audit task. This chapter suggests approaches and guidelines for producing effective internal audit reports developed in hard- or soft-copy format.

Part Five: Impact of Information Technology on Internal Auditing. Internal auditors must know how to evaluate IT controls and to use IT in performing their internal audits. The five chapters in this part outline these important internal audit CBOK areas.

18. **IT General Controls and ITILBest Practices.** The chapter reviews processes for reviewing IT general controls, the controls that cover all aspects of IT operations. In addition, it introduces the Information Technology Infrastructure Library (ITIL), an internationally recognized set of best practices that promote a partnership between business operations and IT functions, and explains why ITIL is important for internal auditors.
19. **Reviewing and Assessing IT Application Controls.** In addition to the general controls covering IT operations, internal auditors need to understand how to review internal controls covering specific applications, ranging from local office desktop procedures to larger enterprise-wide applications. This chapter introduces some internal audit knowledge areas and some IT audit best practices.
20. **Cybersecurity and Privacy Controls.** IT security and privacy issues are major knowledge areas that often require specialized technical skills beyond those of many internal auditors. This chapter introduces some fundamental security and privacy control concepts as well as minimal internal auditor knowledge requirements in this area.
21. **Computer-Assisted Audit Tools and Techniques.** Internal auditors should attempt to audit through the computer when evaluating automated applications and processes. This chapter introduces some computer-assisted audit tools and technique (CAATT) approaches as well as tools for systems auditing.
22. **Business Continuity Planning and IT Disaster Recovery.** Concepts such as backing up major computer files have had a long internal audit history; the objective is to allow restoration of operations in the event of some interruption in IT services. This chapter looks at an expanded view of continuity planning with an emphasis on tools and procedures to get IT operations and the total business back in operation.

Part Six: Internal Audit and Enterprise Governance. The four chapters in this part go beyond just internal audits and discuss the relationship of internal audit with its board audit committee as well as the importance of such areas as ethics procedures and fraud investigations.

23. **Board Audit Committee Communications.** Internal audit reports to the board of directors' audit committees, per SOx rules. While this reporting relationship is very much an audit management responsibility, all internal auditors need to have a better understanding of their roles and responsibilities with regard to the audit committee.
24. **Ethics and Whistleblower Programs.** SOx requirements and other good enterprise governance practices call for ethics and whistleblower programs. The chapter describes many areas in which internal audit can make strong improvement to these operations.
25. **Fraud Detection and Prevention.** Recognizing and detecting fraud is an important internal audit skill. This chapter discusses some basic internal auditing techniques for understanding areas where there may be a danger of fraud.
26. **HIPAA, GBLA, and Other Compliance Requirements.** Numerous U.S. compliance rules impact today's enterprises, such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare-related issues, the Gramm-Leach-Bliley Act (GLBA), and others. This chapter explains some of the more important

of these requirements for enterprise governance and internal audit understanding purposes.

Part Seven: The Professional Internal Auditor. The three chapters in this part focus on professional certifications for internal auditors—important career objectives—as well as internal audit's role as an internal consultant to their enterprise.

27. **Professional Certifications CIA, CISA, and More.** Certifications such as the IIA's Certified Internal Auditor (CIA) are important for building professional credentials. This chapter looks at some of the more important certifications for internal auditors along with their requirements.
28. **Internal Auditors as Enterprise Consultants.** Until very recently, IIA standards prohibited internal auditors from acting as consultants in the same areas where they were performing internal audits. Revised IIA standards now allow an internal auditor to act as a consultant to his or her enterprise. This chapter discusses this new internal audit role and responsibility.
29. **Continuous Assurance Auditing and XBRL.** This chapter discusses two important approaches for internal auditors. Continuous assurance auditing implements audit monitors in usually automated processes to provide audit warnings or trigger signals. XBRL is a coding technique to automate financial statement recorded data such that numerical values on financial reports can be aligned to other internal and external sources. Today's internal auditors should have a knowledge and understanding of both.

Part Eight: Internal Auditing Professional Convergence CBOK Requirements. This final part concludes with chapters on the importance of quality assurance auditing and the impact of International Standards Organization (ISO) standards on internal auditors. In addition, we summarize the chapter-by-chapter materials that together define an internal auditor's CBOK.

30. **ISO 27001, ISO 9000, and Other International Standards.** ISO quality systems standards are becoming increasingly important to enterprises as they operate on a worldwide basis. This chapter discusses the ISO process and reviews some that are important to internal auditors, no matter where they are working.
31. **Quality Assurance Auditing and ASQ Standards.** The more process- and production-oriented American Society for Quality (ASQ) has its own internal audit section with audit procedures that are close to but not the same as IIA internal audit standards. We expect some professional convergence with the IIA and ASQ here going forward. The chapter discusses ASQ internal auditing procedures and their similarity to IIA materials.
32. **Six Sigma and Lean Techniques.** Enterprises worldwide have adopted techniques, such as six sigma, to create operational efficiencies. The chapter looks at several that can be important to internal auditors and considers how some of these programs can be used to enrich and expand internal audit activities.
33. **International Internal Audit and Accounting Standards.** Although the IIA got its start as primarily a U.S.-based organization, it has now expanded to become a truly global professional organization. However, there are some differences in practices and standards as we consider internal auditing on a

worldwide basis. This chapter looks at some important differences in internal auditing and other related global standards. In addition, the chapter discusses the impact of the potential U.S. adoption of the international financial reporting standards (IFRS) internal accounting standards on internal auditors.

34. **CBOK for the Modern Internal Auditor.** This final chapter summarizes the areas where an internal audit should have a strong knowledge as well as others calling for a good general but less specific understanding. The result is a proposed internal audit CBOK.

With this seventh edition, we are taking a stronger and more focused view on the knowledge areas that should be important to today's modern internal auditor. While some topics and issues may change over time, these chapters outline the knowledge areas that are essential to be a successful and outstanding internal auditor today.

About the Author

Robert R. Moeller has over 30 years' experience in internal auditing, ranging from launching new internal audit functions in several companies to providing internal audit consulting and serving as audit director for a Fortune 50 corporation.

Moeller has an MBA in finance from the University of Chicago and an undergraduate degree in engineering; he has accumulated a wide range of professional certifications, including the CPA, CISA, PMP, and CISSP. He served as the national director of information systems auditing for the major public accounting firm, Grant Thornton, where he developed firm-wide audit procedures and directly managed information systems audits, and assumed responsibility for the Chicago office information systems consulting practice.

In 1989 Moeller was recruited to build and organize the first corporate information systems audit function for Sears Roebuck, an organization that then consisted of Allstate Insurance, Dean Witter, and Discover Card, as well as Sears retail and catalog operations. He went on to become their internal audit director, initiating numerous new practices. He has been active professionally in both the Institute of Internal Auditors and the AICPA. He was president of the IIA's Chicago chapter, served on its International Advanced Technology Committee, and was chair of the AICPA's Computer Audit Subcommittee.

In 1996 Moeller launched his own corporation, Compliance and Control Systems Associates, Inc., and presented seminars on internal controls and corporate governance throughout the United States. He was talking about Sarbanes-Oxley issues well before the Act. He helped to launch a new consulting practice for EMC Corporation; has worked as a consultant and project manager, specializing in the telecommunications industry; and has managed a cellular telephone financial system project on a worldwide basis. More recently, he has led a series of Sarbanes-Oxley Section 404 projects in manufacturing, insurance, and other industries. He continues to stay well connected with the overall profession of internal auditing.

Robert Moeller lives with his wife, Lois, in the Chicago area. They enjoy their sailboat on Lake Michigan in the summer, skiing in Colorado and Utah, travel, cooking, and vegetable gardening, and participating in Chicago's theater, opera, and music scene.

PART I

Foundations of Modern Internal Auditing

CHAPTER 1

Foundations of Internal Auditing

The profession of auditing has been with us for a long time. Based on stone documents that have been found, historians have determined that in about 3000 B.C., scribes of Mesopotamian civilizations utilized elaborate systems of internal controls using ticks, dots, and check marks. Auditing has evolved over the millennia, and today we generally think of two basic types of business auditors: external and internal. An external auditor is chartered by regulatory authority to visit an enterprise or entity and to review and independently report the results of that review. In the United States, most external auditors are known as Certified Public Accountants (CPAs), who are state licensed and follow the standards of the American Institute of Certified Public Accountants (AICPA; see aicpa.org). However, there are other types of external auditors in fields such as medical equipment devices, television viewer ratings, and various governmental areas.

Internal auditing is a broader and often more interesting field. As an employee or member of an enterprise, an internal auditor independently reviews and assesses operations in a wide variety of areas, such as accounting office procedures or manufacturing quality processes. Most internal auditors follow high-level standards established by their professional enterprise, the Institute of Internal Auditors (IIA; see theiia.org), but there are many different practices and approaches to internal auditing today due to its worldwide nature and many types of auditing activities.

The prime objective of this book is to define and describe internal auditing as it is performed today—modern internal auditing—and to describe a common body of knowledge (CBOK) for all of internal auditing. Because of its many variations and nuances, we are describing and discussing modern internal auditing in terms of these CBOK, key tools, and knowledge areas that all internal auditors should at least know. These are the common practices that are essential to the profession of modern internal auditing.

An effective first step to begin to understand internal auditing and its key knowledge areas is to refer to its professional organization, the IIA, and its published professional standards. The IIA defines the practice of internal auditing in this way:

> *Internal auditing is an independent appraisal function established within an organization to examine and evaluate its activities as a service to the organization.*

This statement becomes more meaningful when one focuses on its key terms. *Auditing* suggests a variety of ideas. It can be viewed very narrowly, such as the checking of arithmetical accuracy or physical existence of accounting records, or more broadly, as a thoughtful review and appraisal at the highest organizational

level. Throughout this book, the term *auditing* will be used to include this total range of levels of service, from detailed checking to higher level appraisals. The term *internal* defines work carried on within an enterprise, by its own employees, not by external auditors, outside public accountants or other parties, such as government regulators, who are not directly a part of the particular enterprise or enterprise.

The remainder of the IIA's definition of internal auditing covers a number of important terms that apply to the profession.

- The term *independent* is used for auditing that is free of restrictions that could significantly limit the scope and effectiveness of any internal auditor review or the later reporting of resultant findings and conclusions.
- The word *appraisal* confirms the need for an evaluation that is the thrust of internal auditors as they develop their conclusions.
- The term *established* confirms that internal audit is a formal, definitive function in the modern enterprise.
- The phrase *examine and evaluate* describes the active roles of internal auditors, first for fact-finding inquiries and then for judgmental evaluations.
- The term *its activities* confirm the broad jurisdictional scope of internal audit work that applies to all of the activities of the modern enterprise.
- The word *service* reveals that the help and assistance to the audit committee, management, and other members of the enterprise are the end products of all internal auditing work.
- The phrase *to the organization* confirms that internal audit's total service scope pertains to the entire enterprise, including all personnel, the board of directors and their audit committee, stockholders, and other owners.

As a small point, we generally use the term *enterprise* to refer the whole company or business and the term *organization* or *function* to refer to an individual department or unit within an enterprise. In the chapters to come, we describe a variety of other terminology and usage conventions as we discuss a CBOK for modern internal auditing.

Internal auditing should also be recognized as an organizational control within an enterprise that functions by measuring and evaluating the effectiveness of other controls. When an enterprise establishes its planning and proceeds to implement its plans in terms of operations, it must monitor the operations to assure the achievement of its established objectives. These further efforts can be thought of as *controls*. Although the internal audit function is itself one of the types of controls used, there is a wide range of other function-level controls. The special role of internal audit is to help measure and evaluate those other controls. Thus, internal auditors must understand both their own role as a control function and the nature and scope of other types of controls in the overall enterprise.

Internal auditors who do their job effectively become experts in what makes for the best possible design and implementation of all types of controls and preferred practices. This expertise includes understanding the interrelationships of various controls and their best possible integration in the total system of internal control. It is thus through the internal control door that internal auditors come to examine and evaluate all organization activities and to provide maximum service to the enterprise. Internal auditors cannot be expected to equal—let alone exceed—the technical and

operational expertise of the many specialized activities of an enterprise. However, internal auditors can help the responsible individuals achieve more effective results by appraising existing controls and providing a basis for helping to improve those controls. In addition, because internal auditors often have a good knowledge and understanding of many organizational units within a total enterprise, their levels of understanding often exceed that of many other people.

1.1 Internal Auditing History and Background

It is normal for any activity—including a control activity such as internal auditing—to come into being as a result of emerging needs. Although it has ancient roots, internal auditing was not recognized as an important process by many enterprises and their external auditors until the 1930s. This recognition was primarily due to the establishment of the U.S. Securities and Exchange Commission (SEC) in 1934 and changing external audit objectives and techniques at that time. The United States and the rest of the world had just gone through a major economic depression. As a legislative corrective action, the SEC required that enterprises registered with it must provide financial statements certified by independent auditors. This requirement prompted corporations to establish internal auditing departments, the main purpose of which was to assist their independent auditors. At that time, external financial auditors were focusing on expressing an opinion on the fairness of an enterprise's financial statements rather than on detecting internal control weaknesses or even clerical errors. The SEC rules precipitated auditing based on a limited sample of transactions, along with greater reliance on internal control procedures.

Also at that time, internal auditors were primarily concerned with checking accounting records and detecting financial errors and irregularities and often were little more than shadows or assistants to their independent external auditors. Walter B. Meigs, writing about the status of internal auditors during the 1930s, observed that "internal auditors were either clerks assigned to the routine task of a perpetual search for clerical errors in accounting documents, or they were traveling representatives of corporations having branches in widely scattered locations."[1] Early internal auditors were often little more than clerical helpers who carried out routine accounting reconciliations or served as clerical support personnel. Vestiges of this old definition of internal auditing continued in some places even into the early 1970s. For example, in many retail organizations in the late 1960s, the "auditors" were the people who balanced cash registers (remember those?) at the close of the business day.

Although other voices said something should be done to improve and better utilize the potential of internal auditors, things really got started after Victor Z. Brink completed his college thesis on the need for modern internal auditing before he went off to serve in World War II. After the war ended, Brink returned to organize and head internal auditing for Ford Motor, and his college thesis was published as the now long-out-of-print first edition of this *Modern Internal Auditing*.

About that same time period and in 1942, the IIA was launched. Its first membership chapter was started in New York City, with Chicago soon to follow. The IIA was formed by people who had been given the title of internal auditor by their enterprises and who wanted to both share their experiences and gain knowledge with others in this new professional field. A profession was born then that has

undergone many changes over the years and has resulted in the multifaceted profession of modern internal auditor discussed in this book.

The business enterprise of 1940s, when modern internal auditing was just getting started, required a very different skill set than do businesses today. For example, aside from some electromechanical devices and activities in research laboratories, digital computer systems did not exist. Enterprises had no need for computer programmers until computers started to become useful for record-keeping and other computational and accounting functions. Similarly, enterprises had very rudimentary telephone connections; switchboard operators routed all incoming calls to a limited number of desktop telephones. Today, we are all connected through a vast, automated worldwide web of telecommunications and the Internet. The increasing complexity of modern business and other enterprises has created the need for internal auditors to become specialists in various business controls. We can also better understand the nature of internal auditing today if we know something about the changing conditions in the past and the different needs these changes created. What is the simplest or most primitive form of internal auditing and how did it come into existence? How has internal auditing responded to changing needs?

At its most primitive level, a self-assessment or internal auditing function can exist when any single person sits back and surveys something that he or she has done. At that point, the individual asks him- or herself how well a particular task has been accomplished and, perhaps, how it might be done better if it were to be done again. If a second person is involved in this activity, the assessment function would be expanded to include an evaluation of that second person's participation in the endeavor. In a small business, the owner or manager will be doing this review to some extent for all enterprise employees. In all of these situations, the assessment or internal audit function is being carried out directly as a part of a basic management role. However, as the operations of an enterprise become more voluminous and complex, it is no longer practicable for the owner or top manager to have enough contact with all operations to satisfactorily review the effectiveness of enterprise performance. These responsibilities need to be delegated.

Although this hypothetical senior manager could build a supervisory system to try to provide a personal overview of operations, as the enterprise grows larger and more complex, that same manager will find it increasingly difficult to know whether the interests of the enterprise are being properly served. Are established procedures being complied with? Are assets being properly safeguarded? Are the various employees functioning efficiently? Are the current approaches still effective in the light of changing conditions?

The manager must obtain further help by assigning one or more individuals to be directly responsible for reviewing activities and reporting on the types of questions just mentioned. It is here that the internal auditing activity comes into being in a formal and explicit sense. The first internal auditing assignments were usually originated to satisfy very basic and sharply defined operational needs. The earliest special concerns of management was whether the assets of the enterprise were being properly protected, whether company procedures and policies were being complied with, and whether financial records were being accurately maintained. There was also considerable emphasis on maintenance of the status quo. To a great extent, this early internal auditing effort can be viewed as a closely related extension of the work of external auditors.

The result of all of these factors was that the early internal auditors were viewed as playing a narrow role in their enterprises, with relatively limited responsibility in the total managerial spectrum. Their body of knowledge needs was increasing. An early internal auditor was viewed as a financially oriented checker of records and more of a "police officer" than a coworker. In some enterprises, internal auditors had major responsibilities for reconciling canceled payroll checks with bank statements or checking the mathematics in regular business documents. As mentioned, internal auditors in many retail enterprises often were responsible for reconciling daily cash sales to recorded sales receipts.

Understanding the history of internal auditing is important because the old image of internal auditors still exists, to some extent, in various places in the world, even though the character of the internal auditing function is now very different. Over a period of time, the operations of various enterprises increased in volume and complexity, creating managerial problems and new pressures on senior management. In response to these pressures, many senior managers recognized the possibilities for better utilization of their internal auditors. Here were individuals already set up in an enterprise internal audit function, and it seemed possible to get greater value from them with relatively little increase in cost.

At the same time, internal auditors recognized these opportunities and initiated new types of services themselves. Thus, internal auditors gradually took on broader and more management-oriented responsibilities in their work efforts. Because internal auditing was largely accounting oriented at first, this trend was felt first in the accounting and financial control areas. Rather than just report the same accounting-related exceptions—such as some item of documentation lacking a supervisor's initial—internal auditors began to question the overall control processes they were reviewing. Subsequently, internal audit valuation work began to be extended to include many nonfinancial areas in the enterprise.

New business initiatives in the United States, such as the Committee of Sponsoring Organizations (COSO) internal control framework discussed in Chapter 3 or the Sarbanes-Oxley Act (SOx) highlighted in Chapter 4, have caused a continuing increase in the need for the services of internal auditors. In addition, some newer environmental forces have created needs in such areas as protection from industrial hazards, support of quality-control programs, and different levels of business responsibility, including ethical standards. This need for ethical standards includes higher standards for corporate governance, greater involvement of boards of directors and their audit committees, a more active role for stockholders, and greater independence of outside public accountants.

Ethics and social responsibility issues are discussed in Chapter 24. As a result of these new pressures, the services of internal auditors have become more important to all interested parties. There are now more and better-qualified internal auditing personnel and a higher level of enterprise status and importance attached to the position. The IIA has grown from its first, 25-member charter chapter in 1942, to an international association with over 90,000 members and hundreds of local chapters worldwide. At the same time, the importance of internal audit has been recognized by external auditors through their auditing standards, as discussed in Chapter 8. The internal audit profession has reached a major level of maturity and is well positioned for continuing dynamic growth.

Internal auditing today involves a broad spectrum of types of operational activity and levels of coverage. Internal auditing has moved beyond being a staff activity

roughly tied to the controller's department, and internal audit's role is constantly being redefined. SOx has been a major driver of change for internal auditors in the United States and then worldwide. While internal auditors once had a nominal reporting relationship to the board's audit committee, SOx has strengthened and formalized that reporting relationship. However, in some other enterprises, internal audit continues to function at just a routine compliance level. In other situations, internal audit still is integrated too closely with regular accounting activities and limits virtually all of its audit work to strictly financial areas. These exceptions do not reflect the potential capabilities of modern internal auditors. They may also reflect the lack of progressive attitudes in the overall enterprise.

Today, internal audit has expanded its activities to all operational areas of the enterprise and has established itself as a valued and respected part of the senior management effort. The modern internal auditor is formally and actively serving the board of director's audit committee, and the chief audit executive (CAE) today has direct and active level of communication with that same audit committee. This situation reflects major progress in the scope of internal audit's coverage and level of service to all areas of the enterprise. The internal auditing profession itself, through its own self-development and dedication, has contributed to this progress and has set the stage for a continuing upward trend.

1.2 Organization of This Book

The overall object of this book is to define the practice of modern internal auditing as it exists today and to describe a common body of knowledge for the profession. While we generally think of an internal auditor as a professional affiliated with the IIA and its standards, an internal auditor is really a larger, broader person today. Many enterprises have a parallel—almost a shadow—group of quality auditors following the internal audit standards of the American Society for Quality (ASQ; see asq.org). These are internal auditors with different objectives but similar approaches to IIA-background internal auditors; we should see greater convergence between IIA and ASQ internal auditors in the years to come.

The mission and objective of this book and its 34 chapters is to define the practice of modern internal auditing today and to describe an internal audit CBOK. Relying on the internal auditing insights and a heritage, going back to Victor Brink's earliest editions, but with a focus on new and evolving trends and technologies, the chapters of this book are organized in eight parts:

Part One: Foundations of Modern Internal Auditing. Going beyond our discussion on the background of internal auditing discussed here, Chapter 2 discusses the importance of an internal audit CBOK, the expressed needs of the IIA to build such a CBOK, and similar experiences in other professions. In addition, we summarize our chapter-by-chapter CBOK elements.

Part Two: Importance of Internal Controls. The review and understanding of internal control is a major internal audit strength. Chapters in this part discuss the COSO's internal control framework and the internal control aspects of the SOx. Our SOx material highlights the new external auditing standards, called Auditing Standard No. 5 (AS 5). In addition, we highlight

the importance of what is known as the *C*ontrol *ob*jectives for *i*nformation and related *T*echnology (CobiT) framework as a vehicle for understanding internal controls.

Part Three: Planning and Performing Internal Audits. This part covers the overall process of performing internal audits with an introduction of the international IIA's internal auditing standards and guidelines for performing effective internal audits. Chapters here discuss the process of assessing and evaluating audit evidence as well as documenting audit results, with an emphasis on electronic flowcharts and workpapers.

Part Four: Organizing and Managing Internal Audit Activities. An effective internal audit function requires a well-planned and organized audit function that selects appropriate areas for audit, based on their relative risk. Chapters in this part discuss approaches to building an effective internal audit organization, understanding key competency needs, and risk-based audit planning. Chapters also discuss the very important area of project management as well as process modeling for internal auditors. This part includes the very important area of reporting internal audit results.

Part Five: Impact of Information Systems on Internal Auditing. Information systems or information technology (IT) has a major impact on the areas where internal auditors perform reviews as well as tools to assist the internal audit process. The five chapters in this part describe procedures for internal audit reviews of IT controls on multiple levels. IT-related security and continuity planning procedures are discussed, as well as computer-assisted audit tools and techniques (CAATTs) to help perform more effective internal audits.

Part Six: Internal Audit and Enterprise Governance. Internal audit has a major role today in helping to build a more effective corporate governance environment. This includes understanding and monitoring compliance with many of the new rules that enterprises face today, helping to build a better ethics atmosphere, and focusing some audit work on fraud detection and prevention. Perhaps most important, Chapter 23 in this part discusses how internal audit can better serve and assist the audit committee of the board of directors.

Part Seven: The Professional Internal Auditor. The professional designations of Certified Internal Auditor (CIA) and Certified Internal Systems Auditor (CISA) are very important for internal audit professionals. Chapter 27 discusses the requirements of these as well as some other important internal auditor professional achievements. In addition, other chapters in this part introduce the advanced auditing technique of continuous assurance auditing as well as the role of internal auditors as internal enterprise consultants.

Part Eight: Internal Auditing Professional Convergence CBOK Requirements. This part looks at the ASQ internal audit process, reviews of quality systems standards, and techniques such as six sigma. This part and the book conclude with an introduction to worldwide audit standards, our CBOK, and the future modern internal auditor.

The chapters in this edition define a professional internal auditor CBOK and discuss the roles and responsibilities of today's modern internal auditor. Even though

past editions covered a wide range of areas, in this volume, subjects and topics have been organized with this internal audit CBOK as a theme. It is our objective that the materials in the chapters to come will help all internal auditors to gain knowledge and expertise in their profession and for management and others to better understand the practice of modern internal auditing.

Note

1. Walter B. Meigs, *Accounting Review* 35, No. 2 (April 1960): 377.

CHAPTER 2

Internal Audit's Common Body of Knowledge

Internal audit professionals constantly encounter areas where they are expected to gain personal and professional knowledge to assist them in performing internal audits. These knowledge areas come from industry developments, standards changes introduced by the Institute of Internal Auditors (IIA) or others, technology changes such as use of new Internet Web services, or just good ideas developed from other internal auditors following the IIA's "Progress through Sharing" motto. Some of this internal audit knowledge comes from learning more about industry-specific regulatory requirements; others are just good ideas to make internal audits more effective and efficient. The bottom line, though, is that internal auditors at all levels are expected to have knowledge in a wide variety of areas, some unique to an individual enterprise or product area while others cover the general practice of internal auditing. There are many knowledge area needs, and a new internal auditor might ask, "What do I need to know to become an experienced, qualified, and well-respected internal auditor?"

Over time, experienced internal auditors have given different answers to this type of question. Victor Brink, in the first 1945-era edition of this book, introduced a variety of important internal audit knowledge areas, and that was before the days of information technology (IT), the Internet, and the massive changes in world businesses over the last 50-plus years. Other authors have tried to define internal auditor knowledge requirements over the years, and this author certainly tried to explain many internal audit knowledge areas in the prior two editions of this book. However, there has been no recognized minimal set of internal audit knowledge requirements. That is, there has been no published common body of knowledge (CBOK) for the professional of internal auditing.

This lack of a CBOK for the professional practice of internal auditing was frequently emphasized by William G. Bishop III, CIA (Certified Internal Auditor), who served as president of the IIA from 1992 until his untimely death in 2004. Subsequent to Bishop's death, the IIA recognized this need for a CBOK for the profession and contracted with a team of researchers to help define such a CBOK for internal auditing. The results of their efforts to date are discussed in Section 2.2.

Given its historical background and ongoing attempts to describe all aspects of the profession of internal auditing, we have described "A Common Body of Knowledge" as the major theme of this edition. The chapters that follow describe the major or common knowledge requirements of today's modern internal auditor;

some of these are areas where an internal auditor must have a strong knowledge and understanding. Others are areas where an internal auditor should develop a good general awareness. An example of the former is Chapter 8 on internal audit professional standards, an essential internal audit knowledge area. Other topics, such as Chapter 32 on six sigma and lean techniques, cover areas where an internal auditor should have a good general awareness. Taken together, however, all of these chapters define an internal auditing common body of knowledge.

2.1 What Is a CBOK?: Experiences from Other Professions

Business and professional terms and acronyms often get used and reused so often that we sometimes really miss their true meanings. The expression "common body of knowledge" falls in that category. A CBOK for any profession defines the minimum level of proficiency needed for effective performance within that profession. Rather than embodying all the knowledge domains that a practitioner, such as an internal auditor, might need to be viewed as an "expert" in that profession, a CBOK focuses on the *minimal* knowledge needed by any professional in that discipline to perform effectively.

A Web search for "CBOK" on Google or other search engines gives references to multiple professional organizations that have developed or attempted to develop their own CBOKs. For example, the Bank Administration Institute (BAI; www.bai.org) has released a CBOK for banking industry risk professionals. With risk management an important knowledge area of banking, the BAI felt that a CBOK was necessary to define knowledge needs and expectations for banking professionals specializing in that area. Knowledge and an understanding of the areas described in this CBOK have enhanced the professional credibility of some professionals. Sometimes, however, the development of a CBOK started as a good idea that fizzled out for lack of funding or interest. The once-prominent Institute for the Certification of Computer Professionals (ICCP)[1] attempted to develop its own IT-oriented CBOK, but IT processes and knowledge areas perhaps moved faster than any group was able to document and describe. Never really fully launched, the ICCP CBOK is little more that a historical footnote on the Web today.

Other professional organizations have tacked the "BOK" suffix to a set of practices common to their profession. For example, the Project Management Institute (PMI) has published a set of knowledge requirements for project managers, calling this material their *PMBOK*® (see www.pmi.org). Many specialized professional organizations have tried to capture all of the terms or concepts that a professional operating in that field should know. Even the U.S. Department of Homeland Security has developed an IT-based security standard that it calls the Essential Body of Knowledge (EBK).[2]

The formats of these BOK documents vary. Some are little more than fairly general outlines; others are very detailed descriptions of the knowledge areas where a professional will be expected to have some skills or to operate. The PMI's *PMBOK*® is a good example of what a professional should expect in a book of knowledge compendium. The guide breaks down all elements of the project management process, describing inputs, tools and techniques, and then outputs for each element. The elements are then linked to other activities in the project management process. A knowledge or understanding is an important internal audit skill, whether

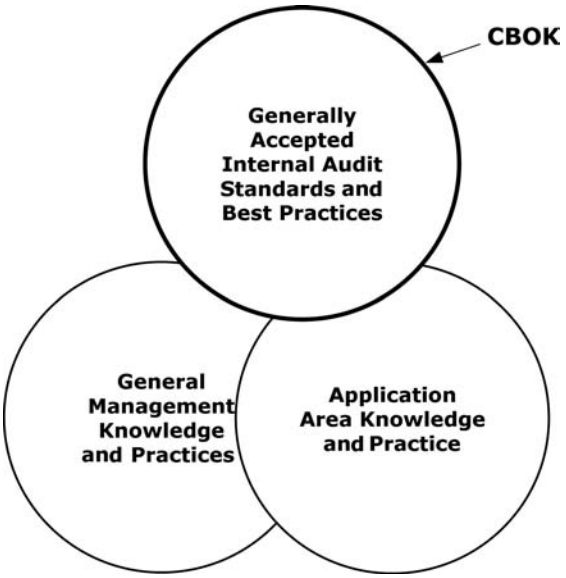


EXHIBIT 2.1 Relationship of a CBOK to Other Knowledge Areas

it is planning a comprehensive plan of internal audits over the year or outlining the requirements and tasks for a specific audit. Chapter 14 references the PMI's *PMBOK* as part of an internal audit CBOK knowledge requirement area.

Any type of published CBOK cannot just stand by itself, no matter how detailed any description. For internal auditors, a CBOK will cover a wide variety of internal audit–specific practice areas but must be linked with general management knowledge and practice disciplines as well as application knowledge areas, as shown in Exhibit 2.1. This same concept should be considered for all published bodies of knowledge.

2.2 Institute of Internal Auditor's Research Foundation CBOK

Chapter 1 highlighted some of the origins of internal auditing and discussed how the profession has evolved from one of primarily accounting support and mathematical-accuracy checkers to today's internal control evaluation specialists. The profession has come a long way. Following the IIA's *International Standards for the Practice of Internal Auditing,* described in Chapter 8, internal auditors today are working in corporate, not-for-profit, and governmental agencies worldwide. In addition, they are working in all sizes of enterprises, in all industry areas, and under many different conditions. Despite all of these varied conditions, however, there is or should be a wide range of common internal audit practices.

Beyond these IIA standards and some legal requirements for internal audit reviews, there are not many defined rules of right and wrong guidance for internal audit practices. Rather, internal auditors today follow a whole range of best practices under the overall guidance of the IIA standards. Many internal audit best practices have been communicated from one internal auditor to another through IIA

publications and activities, following their "Progress through Sharing" motto. However, over the years, internal audit professionals have expressed a need to better formalize things and develop an internal audit CBOK. Although there had been several limited attempts to develop such a body of knowledge, the IIA Research Foundation (IIARF) launched a major effort in 2006 to develop such a CBOK for the internal audit profession. Its preliminary result, dated 2008, was published in a mid-2007 research study.[3]

The stated objective of this survey was to capture and describe the state of the internal auditing professional practices throughout the world including:

- The knowledge and skills that internal auditors possess
- The skill and organizational levels used for the practice of internal auditing work
- The actual duties performed by internal auditors
- The structure of internal audit organizations
- The types of industries which practice internal audit
- The regulatory environment of various countries

The IIARF CBOK had a stated objective of documenting the understanding of the unique value-added role that internal auditing has in enterprises throughout the world. Based on this understanding, an objective of the IIARF CBOK was to better define the future of internal auditing and ensure that it remains a "vibrant and relevant contribution to enterprises." The IIA has stated it plans to use the results of this 2007 study to improve future standards, procedures, and other offerings in areas including revised internal audit certifications and examinations, revised standards, and other internal audit publications.

The IIARF's CBOK objectives, however, were not to develop a set of high-level standards for performing internal audits, such as the approach used in the PMI's *PMBOK* (discussed further in Chapter 14) or the Information Technology Infrastructure Library (ITIL) best practices (see Chapter 18). Rather, the IIARF aimed just to gain a better knowledge of the current duties and activities of internal auditors in various IIA chapter units worldwide and as individuals operating as heads of internal audit functions including chief audit executives (CAEs), audit managers, internal audit seniors/supervisors, staff members, and others affiliated with internal audit.

Although called a CBOK, the IIARF's approach was not to define any set of internal audit common knowledge best practices but to survey what internal auditors were doing at the time of the study's publication in country-by-country practices of internal auditing. To develop the IIARF study, a team of contractors was engaged, a standard detailed surveys form was developed, and these surveys were sent to some 9,000 individual internal audit functions. The summarized results provided a view of what internal audit departments—what the IIARF CBOK document calls Internal Auditing Activities (IAAs)—are doing as part of their internal audit work. Although the IIARF reports that all results have been captured in a detailed database, initial published results provide only a high-level look at these survey responses. Significantly, there is no split between IIARF CBOK's defined IAAs at larger enterprises, such as those in the United States and the United Kingdom, and those in the many smaller country and enterprise internal audit functions worldwide.

The IIARF CBOK surveys were assembled similar to a consumer-type survey where participants were asked to respond to questions based on a score ranging

from 1 to 5 for each question. That is, a response of 5 meant the respondent strongly agreed to a survey question, 4 was just agreed, and a score of 1 indicated the respondent strongly disagreed. The results were published as a single mean value of the various responses; no standard deviation values showed the ranges of those responses. For example, the CBOK study contained this evaluation statement: "Your internal audit activity brings a systematic approach to evaluate the effectiveness of internal controls." A reported 2,374 CAEs responded to this question with a mean value of 4.35. One would have expected a response of nearly 5.0 here; does this mean that some internal audit functions *do not* follow a systematic approach in their reviews of internal controls? If true, these could be disturbing results.

Another problem with this type of reported result is that we really do not have any further information to support these types of responses or the variances in the reported scores. While the CAE for an effective internal audit function would be expected to respond to such a question with a score of 5.0, the published IIARF CBOK does not explain why a certain number of CAEs did not strongly agree with the question. Is it because a certain portion of internal audit functions are not that effective, or because of people's natural tendency not to score surveys on the total high or low end of the range? This is a problem with many of IIARF CBOK's reported responses. Almost all scores are reported as somewhat greater than 4.0 but less than 5.0. These three IIARF CBOK evaluation statements were ranked under 4.0 but above 3.5:

1. Your internal audit activity brings a systematic approach to evaluate the effectiveness of governess processes.
2. The way our internal audit activity adds value to the governance process is through direct access to the audit committee.
3. Compliance with the IIA's *Standards for the Professional Practice of Internal Auditing* is a key factor for your internal audit activity to add value to governance processes.

With all levels of respondents reporting relatively low scores for these questions, some internal audit management concerns should be apparent here. Of course, decoding responses to these types of statements is always a concern. For example, for the second statement, do respondents' answers mean that many do not feel their internal audit activities add value to their enterprise's governance activities, that they do not have sufficient access to their audit committees, or both?

This IIARF CBOK study is filled with tables showing—based on the survey responses—what internal audit functions are doing across the world. If nothing else, this type of reported information will allow a CAE to assess if his or her internal audit function is performing activities in line with other internal audit functions worldwide. We have extracted the results from two of CBOK's published table results, but the interested reader should contact the IIARF for a copy of the recently published CBOK results.

As an example of the IIARF's CBOK reported materials, Exhibit 2.2 shows the relative internal audit usage, ranked both overall and by level of internal auditor, for a series of common internal audit tools and techniques. The IIARF CBOK selected 16 internal audit tools and techniques and ranked them by utilization. These important tools and techniques will be the basis for many of our chapters. Not unexpectedly, the Internet and related e-mail processes were found to be the most important of

EXHIBIT 2.2 Internal Audit Tools and Techniques Ranked by Overall Usage

Tools and Techniques	Overall	CAE	Audit Manager	Senior/ Supervisor	Audit Staff	Others
Internet Web and E-mail	1	1	1	1	1	1
Risk-Based Audit Planning	2	2	2	2	2	2
Analytical Reviews	3	3	4	3/4	4	3
Electronic Workpapers	4	4	3	3/4	3	4
Statistical Audit Sampling	5	5	6	5	5	5
Computer-Assisted Audit Techniques	6	6	5	6	6	6
Flowchart Software	7	7/8	7	7	8/9	7/8
Benchmarking	8	7/8	8	9/10	11	7/8
Process Mapping Applications	9	9	9	8	8/9	7/8
Control Self-Assessments	10	1	10	9/10	10	9
Data Mining	11	10	11	12	12	12
Continuous/Real-Time Auditing	12	12	13	11	7	11
IIA Quality Assessment Review Tools	13	13	12	14	14	14
Balanced Scorecard	14	14	14	13	15	15
Total Quality Management Techniques	15	15	15	15	13	16

Source: Based on Table 2-6 from the IIA's 2006 CBOK survey.

these internal auditing tools and techniques. Process modeling software was ranked in a middle range here, but this is not surprising as process modeling software and the supporting notations for its use are difficult for many people to use and are somewhat complex. The lowest ranked internal audit tool and technique here, total quality management, was surprising. The IIA has emphasized quality management processes very much over recent years and built it into its standards. Chapter 31 discusses the importance of quality assurance auditing procedures.

As another example of the IIARF CBOK materials, Exhibit 2.3 contains a series of survey statements directed to CAEs and to internal audit managers asking if the statement currently applies to their internal audit function, whether they will likely install the practice in the future, or if it is not applicable or planned. While some of these survey questions would not apply to some not-for-profit and other internal audit groups, many of these results here are surprising. For example, to the statement "Internal audit has implemented an internal control framework," only about 70% of internal audit managers responded that they have such an internal control evaluation process currently in place; the bulk of the others planned to do something within the next three years. With IIA standards calling for such activities to be in place in order to be an effective and compliant internal audit function, much more work appears needed. Chapters 3 through 6 discuss the importance of internal controls and a framework for establishing and measuring them. Beyond the tables extracted here, the IIARF CBOK is filled with other interesting and sometimes perhaps disturbing observations.

Some of the IIARF CBOK published responses are professionally disturbing on several levels. For example, only some 82% of all IIARF CBOK respondents state that they use IIA standards in whole or in part. These are the ground rules for internal auditing, and one really wonders about the nearly 20% who say they do not use these standards, even in part. Chapter 8 discusses the importance of IIA standards.

EXHIBIT 2.3 Internal Audit Management Agreement to IIARF CBOK Survey Statements

Statement	Number of Respondents	Currently Applied (%)	Likely to Apply within Next 3 Years (%)	Will Not Apply in Foreseeable Future (%)	Not Applicable (%)
Internal audit is required by law or regulation where the enterprise is based.	3,464	61.2	43.1	12.9	12.8
Internal auditors have an advisory role in enterprise strategy development.	3,445	28.9	32.7	30.3	8.0
Internal audit complies with a corporate governance code.	3,447	67.7	22.7	4.3	5.3
Internal audit has implemented an internal control framework.	3,443	70.5	24.3	3.5	1.7
Internal audit has implemented a knowledge management system.	3,423	25.6	43.9	20.6	9.9
The internal audit function has provided training to audit committee members.	3,424	34.0	32.3	18.5	15.1
Internal audit assumes an important role in the integrity of financial reporting.	3,437	55.7	25.6	13.7	4.9
Internal audit educates enterprise personnel regarding internal controls, corporate governance, and compliance issues.	3,437	64.3	25.3	7.3	3.1
Internal audit places more emphasis on assurance activities rather than on consulting activities.	3,448	71.5	15.2	844.0	4.9

Source: Findings extracted from Table 2-14 from the IIARF's 2006 CBOK study.

The IIA has stated that it plans to update the IIARF CBOK study every three years and has expressed general plans to develop and release other products and offerings to enhance and build this internal audit CBOK. During the IIA's 2008 international conference, however, no sessions on the status on the IIARF CBOK study were included in the technical program. In light of the need for a better definition of internal audit's knowledge requirements, this new edition of *Brink's*

Modern Internal Auditing was very much motivated by the IIARF CBOK study. There is a need for an internal audit CBOK that defines the wide range of activities where internal auditors need skills and understanding, and our major objective is to outline such an approach.

The IIARF's CBOK is not a guide to internal auditor best practices. Rather, it describes a wide range of internal audit activities and how they are practiced. The CAE as well as the audit committee and management responsible for internal audit within an enterprise should view this IIARF CBOK as somewhat of a wake-up call regarding how individual internal audit groups are performing. In general, the IIARF CBOK points out many areas where an internal audit function should improve.

An individual CAE should not use the IIARF CBOK reported findings as a justification for current inaction, saying that because some practice is not being followed this can be justified because only a less than majority X% of others are doing it as well. Rather, these IIARF CBOK findings should highlight areas where improvements are needed in individual internal audit areas and in standard requirements. For example, the IIARF CBOK reported that over 50% of internal audit functions worldwide were not in compliance with a requirement for a periodic external third-party review. Perhaps this means that the standard needs some rethinking or revision. As all internal auditors should know, when reviewing compliance in some area, a finding the "everybody does it" is not an excuse for an internal control failure or some other failure. Rather than the approach for issuing Sarbanes-Oxley (SOx) auditing rules, discussed in Chapter 4, with little chance to review or comment, the IIA's standards are established through a volunteer committee effort. Through their local IIA chapters, internal auditors should get more involved with the development process. More important, these IIA standards effectively define the body of knowledge or sets of best practices for internal auditing. The IIA's international *Standards for the Professional Practice of Internal Auditing* will be the basis of our CBOK for today's internal auditors.

2.3 What Does an Internal Auditor Need to Know?

Does every internal auditor need to have a detailed understanding of all of the topics summarized in the preface to this book? We would argue an answer of no, but we feel every internal auditor should develop of general understanding of essentially all of the issues and topics discussed in this book. Some of these areas may be specialized, but an internal auditor must have at least awareness of them. For all internal auditors, and especially for new internal auditors, materials such as the Committee of Sponsoring Organizations (COSO) framework for internal controls, discussed in Chapter 3, are essential, as are Chapter 7's discussion of planning and performing internal audits and Chapter 8's discussion of the IIA internal audit standards. Other chapter topics may only point to areas where internal auditors can gain some support information. However, newer internal auditors can use this material to gain a better understanding of the depth and breadth of modern internal auditing.

More experienced internal auditors generally specialize in some areas and have greater levels of specific industry knowledge. Whether the enterprise manufactures heavy industrial equipment or provides some type of financial services, an experienced internal auditor should develop skills and knowledge of those specific

areas. This knowledge can come from reading industry-specific publications, attending trade shows, or just listening, listening and more listening. After gaining that industry-specific knowledge, an internal auditor should be able to use some of that knowledge to merge with internal audit principles, as appropriate, discussed in the chapters that follow.

This book aims to provide internal auditors at all levels with an understanding—albeit sometimes just a very general understanding—of some of the many topic areas that impact the profession of internal auditing. When encountering a topic such as ITIL internal control concerns, for example, a reader should be able to return to the index of this book and find some general information on ITIL (discussed in Chapter 18) as well as some ITIL-related internal audit issues.

2.4 Modern Internal Auditing's CBOK Going Forward

We recognize that the field and profession of internal auditing is broad. This book tries to cover only what we feel are perhaps some of the most important knowledge areas for today's modern internal auditor. Our discussion on the recent IIARF CBOK survey highlighted a variety of internal audit practice areas that we do not include in our discussion of a CBOK for internal auditing. For example, the IIARF CBOK study mentions "Emerging Markets" and "Globalization" as two potential but highly scored emerging issues. Perhaps that will be the case; we chose not to discuss these areas.

The IIA has announced major plans to build and expand on its IIARF CBOK study in the years to come. However, as their recently published IIARF CBOK found a fairly significant number of internal auditors currently are not even following IIA standards, the IIA may review these findings and just issue more basic educational material going forward. These reported practices show a real internal auditor knowledge need.

Notes

1. The organization, at www.iccp.org, was one of the early proponents of testing and certifying IT professionals through its Certificate in Data Processing program from the 1970s. It attempted to develop a CBOK for computer professionals, but the project evidently ran out of steam in the late 1990s.
2. *Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development,* U.S. Department of Homeland Security (September 2008), www.ITSecurityEBK@dhs.gov.
3. Institute of Internal Auditors Research Foundation, *A Global Summary of the Common Body of Knowledge* (Altamonte Springs, FL: 2007).

PART II

Importance of Internal Controls

CHAPTER 3

Internal Control Framework: The COSO Standard

Understanding and implementing effective internal controls is a basic principle of internal auditing. A system of internal controls has and continues to be the basis for effective operational and accounting business processes, and a major internal auditing activity involves evaluating and assessing multiple levels of controls. External auditors have preferred the term *internal control,* and internal auditors often refer to just *controls.* The concept has been a major activity and concern for internal auditors and business managers. However, it is one of those good-sounding expressions that did not have any consistent definition or use prior to the 1970s, when a series of events in the United States led to the development and release of the Committee of Sponsoring Organizations (COSO) internal controls framework. First recognized for assessing internal controls by U.S. external auditors and then as the standard for building and measuring internal controls under the Sarbanes-Oxley Act (SOx), the COSO internal controls framework has become the worldwide standard for building and assessing internal controls. A general understanding of the COSO internal controls framework and its elements is a key common body of knowledge (CBOK) requirement for all internal auditors.

This chapter briefly discusses "how we got there"—the activities by auditors, regulators, and other professionals over the years to develop a consistent approach to defining and understanding internal controls leading to this COSO framework. The COSO internal controls framework is an essential tool for understanding internal controls and for assessing compliance with SOx internal accounting control requirements. It should be noted that there are two different COSO frameworks. The first—the emphasis of this chapter—COSO internal controls provide a consistent definition for this important concept, sometimes just called the COSO framework. However, after SOx became effective in 2004, COSO also released an enterprise risk management framework called COSO ERM (see Chapter 6). Although COSO ERM sometimes looks similar to the original COSO internal controls framework, it describes different areas and objectives. Throughout this book, we use both *COSO ERM* and the *COSO internal controls framework.*

3.1 Importance of Effective Internal Controls

Internal control is one of the most important and fundamental concepts that business professionals at all levels and both external and internal auditors must understand.

Business professionals build and use internal controls; auditors review both operational and financial areas in the enterprise with an objective of evaluating their internal controls. Internal and external auditors have many different objectives. Most references to auditors in this chapter apply to internal auditors, who have a major responsibility to understand and assess COSO internal controls. Although there have been many slightly different definitions of internal controls in the past, our definition is:

> *Internal controls are processes, implemented by management, that are designed to provide reasonable assurance for:*
>
> - *Reliable financial and operational information*
> - *Compliance with policies and procedures plans, laws, rules, and regulations*
> - *Safeguarding of assets*
> - *Operational efficiency*
> - *Achievement of an established mission, objectives and goals for enterprise operations and programs*
> - *Integrity and ethical values*

This definition recognizes that internal control extends beyond just accounting and financial matters and includes all enterprise processes. An enterprise unit or process has good internal controls if it (1) accomplishes its stated mission in an ethical manner, (2) produces accurate and reliable data, (3) complies with applicable laws and enterprise policies, (4) provides for economical and efficient uses of resources, and (5) provides for appropriate safeguarding of assets. All members of an enterprise are responsible for the internal controls in their area of responsibility and for operating them effectively.

Despite or perhaps because of this broad and wide-reaching internal controls definition, many business professionals have had problems in fully understanding and applying internal control concepts. The concept of an internal control and supporting control processes goes back to the basic mechanical and paperwork procedures that once existed throughout everyday life. Control processes are necessary for activities inside and outside today's enterprise, and many basic concepts and principles are the same no matter where the control is implemented. An automobile provides some basic controls examples. When the accelerator—a speed control—is pressed, the automobile goes faster. When the brake—another control—is depressed, the automobile slows or stops. When the steering wheel is turned, the vehicle turns. The driver *controls* the automobile, and all three of these represent the car's basic internal control system. If the driver does not use or improperly uses the accelerator, brake, or steering wheel, the automobile will operate *out of control*.

Expanding this concept just a bit, a stop sign, traffic direction sign, or gate crossing barriers all represent external controls to the auto and its driver. The driver is the operator of the automobile-based internal control process or system but has little decision authority over the message delivered from a traffic light external control.

From an internal control perspective, an enterprise can be compared to our automobile example as well. There are many enterprise systems and processes at work, such as accounting operations, sales processes, and information technology

(IT) systems. If management does not operate or direct these processes properly, the enterprise may operate out of control. All members of an enterprise should develop an understanding of the appropriate control systems in their areas or responsibility and then determine if they are operating properly connected in their area of enterprise operations. These are referred to as the enterprise's *internal control* systems.

To clear up just a small point of ambiguity, although the professional literature for external auditors uses the term *internal control*, internal audit standards call the same concept a *control*. For purposes of this book and for internal auditors professionally, they both mean the same thing. The Institute of Internal Auditors (IIA) *International Standards for the Practice of Internal Auditing*, discussed in Chapter 8, define controls as:

> *Any action taken by management, the board, and other parties* to manage *risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.*[1]

Management is responsible establishing and managing those controls, and Internal auditors both assess their effectiveness and make recommendations as appropriate.

3.2 Internal Controls Standards: Background

Although the concept and definition of internal controls is fairly well understood today with the COSO internal control framework, this was not true before the late 1980s. In particular, there was no consistent agreement of what was meant by "good internal controls." Early definitions that first came from the American Institute of Certified Public Accountants (AICPA) and were used by the U.S. Securities and Exchange Commission (SEC) for the Securities Exchange Act of 1934 regulations provide a good starting point. Although there have been changes over the years, the AICPA's first codified standards, called the Statement on Auditing Standards (SAS No. 1), defined the practice of financial statement external auditing in the United States for many years. It used this definition for internal control:

> *Internal control comprises the plan of enterprise and all of the coordinate methods and measures adopted with a business to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies.*

That original AICPA SAS No. 1 was modified to add administrative and accounting controls to the basic internal control definition. Administrative control includes, but is not limited to, the plan of enterprise and the procedures and records that are concerned with the decision processes leading to management's authorization of transactions. Such authorization is a management function directly associated with the responsibility for achieving the objectives of the enterprise and is the starting point for establishing accounting control of transactions.

[Accounting control] comprises the plan of enterprise and the procedures and records that are concerned with the safeguarding of assets and the reliability of financial records and consequently are designed to provide reasonable assurance that:

a. *Transactions are executed in accordance with management's general or specific authorization.*
b. *Transactions are recorded as necessary (1) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statement and (2) to maintain accountability for assets.*
c. *Access to assets is permitted only in accordance with management's authorization.*
d. *The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.*[2]

The overlapping relationships of these two types of internal control were then further clarified in these pre-1988 AICPA standards:

The foregoing definitions are not necessarily mutually exclusive because some of the procedures and records comprehended in accounting control may also be involved in administrative control. For example, sales and cost records classified by products may be used for accounting control purposes and also in making management decisions concerning unit prices or other aspects of operations. Such multiple uses of procedures or records, however, are not critical for the purposes of this section because it is concerned primarily with clarifying the outer boundary of accounting control. Examples of records used solely for administrative control are those pertaining to customers contacted by salesmen and to defective work by production employees maintained only for evaluation personnel per performance.

Our point here is that the definition of the term *internal control* has changed but been reinterpreted over the years. However, the earlier AICPA standards stress that the system of internal control extends beyond just matters relating directly to the accounting and financial statements, including administrative controls. Over the years up through the 1970s, the SEC and the AICPA released many often slightly differing internal control definitions and the major external auditing firms provided voluminous supporting interpretations and guidelines.

(a) Internal Control Definitions: Foreign Corrupt Practices Act of 1977

Just as the accounting scandals of Enron and others brought us SOx in the early years of the twenty-first century, the United States experienced a similar situation some 30 years ago. The period from 1974 to 1977 was a time of extreme social and political turmoil in the United States. A series of illegal acts were discovered at the time of the1972 U.S. presidential election, including a burglary of the Democratic party headquarters in a building complex known as Watergate. The events eventually

led to the resignation of President Richard Nixon. Related investigations found other questionable practices had occurred that were not covered by legislation. Similar to how the failure of Enron brought us SOx, the result here was passage of the 1977 Foreign Corrupt Practices Act (FCPA).

The FCPA prohibited bribes to foreign—non-U.S.—officials and also contained provisions requiring the maintenance of accurate books and records as well as systems of internal accounting control. With provisions that apply to virtually all U.S. companies with SEC-registered securities, the FCPA's internal control rules particularly impacted both internal and external auditors. Using terminology taken directly from the legislation, the FCPA required that SEC-regulated enterprises must:

- *Make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuers.*
- *Devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that:*
  - *Transactions are executed in accordance with management's general or specific authorization.*
  - *Transactions are recorded as necessary both to permit the preparation of financial statements in conformity with generally accepted accounting principles (GAAP) or any other criteria applicable to such statements, and also to maintain accountability for assets.*
- *Access to assets is permitted only in accordance with management's general or specific authorization.*
- *The recorded accountability for assets is compared with the existing assets at reasonable intervals, and appropriate action is taken with respect to any differences.*

The FCPA was significant because, for the first time, management was made responsible for an adequate system of internal accounting controls. The act required enterprises to "make and keep books, records, and accounts, which in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer." Similar to and even broader than today's SOx rules discussed in Chapter 4, the FCPA record-keeping requirements applied to all public corporations registered with the SEC.

In addition, the FCPA required that these enterprises keep records that accurately reflect their transactions "in reasonable detail." While there was no specific definition here, the intent of the rule was that records should reflect transactions in conformity with accepted methods of recording economic events, preventing off-the-books "slush funds" and payments of bribes. The FCPA required that companies maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are authorized and recorded to permit preparation of financial statements in conformity with GAAP. Also, FCPA rules stated that accountability is to be maintained for an enterprise's assets, and access to them permitted only as authorized with periodic physical inventories. Passed over 30 years ago, the FCPA was a strong set of corporate governance rules. Because of the FCPA, many boards

of directors and their audit committees then began to actively review the internal controls in their enterprises.

(b) FCPA Aftermath: What Happened?

When enacted, the FCPA resulted in major efforts to assess and document systems of internal controls in major U.S. corporations. Enterprises that had never formally documented their internal control procedures embarked on major compliance efforts. Often this FCPA documentation responsibility was given to internal audit departments, which used their best efforts to comply with the FCPA's internal control provisions. Recall that this was in the late 1970s and very early 1980s; at the time, most automated systems were mainframe batch-oriented processes, and available documentation tools were little more than plastic flowchart templates and No. 2 pencils. Similar to the first days of SOx Section 404 (see Chapter 4), corporations went through considerable efforts to achieve FCPA compliance. Many large enterprises developed extensive sets of paper-based systems documentation but made no provisions, once they had been completed, to update them regularly.

Many business professionals anticipated a wave of additional regulations following the FCPA's enactment. However, this did not occur. Legal actions were essentially nonexistent, no one came to inspect the files of assembled documentation that were mandated in the FCPA legislation, and today the FCPA has dropped off our radar screen of current "hot" management topics. The FCPA is still in force but today as more of an anticorruption, antibribery law. A Web search will yield few if any references to the FCPA's internal control provisions. The law was amended in the 1990s but only to strengthen and improve its anticorruption provisions.

When enacted in 1977, the FCPA emphasized the importance of effective internal controls even though there was no consistent definition of internal controls at that time. However, the FCPA heightened the importance of internal controls, and its antibribery provisions continue to be important. The FCPA was an important first step for helping enterprises to think about the need for effective internal controls, even though there were no guidelines or standards over the FCPA's systems documentation requirements. Nevertheless, if there had been more attempts at FCPA internal controls compliance documentation, we might never have had SOx.

3.3 Events Leading to the Treadway Commission

Despite the FCPA requirements for documenting internal controls, it soon became obvious that no clear and consistent understanding of what was meant by "good internal controls" existed. In the late 1970s, external auditors only reported that an enterprise's financial statements were "fairly presented"; there was no mention of the adequacy of the internal control procedures supporting those audited financial statements. The FCPA required the reporting enterprises to document their internal controls but did not ask external auditors to attest to whether an enterprise was in compliance with the FCPA's internal control reporting requirements. The SEC then began a study on internal control adequacy and issued a series of reports over a 10-year period to better define both the meaning of internal control and the external auditor's responsibility for reporting on those controls.

In 1974, the AICPA formed a high-level Commission on Auditor's Responsibilities. This group, better known then as the Cohen Commission, recommended in 1978 that a statement on the condition of an enterprise's internal controls should be required along with their financial statements. Although these Cohen Commission recommendations occurred at about the same time as the release of the FCPA, they ran into a torrent of criticism. In particular, the report's recommendations were not precise on what was meant by "reporting on internal controls," and external auditors expressed strong concerns regarding their roles in this process. External auditors were concerned about potential liabilities if their reports on internal control gave inconsistent signals due to a lack of understanding over the definition of internal control standards. Although auditors were accustomed to attesting to the fairness of financial statements, the Cohen Commission report called for an audit opinion on the fairness of the management control assertions in the proposed financial statement internal control letter. Again the issue was raised that management did not have a consistent definition of internal control. Different enterprises might use the same terms regarding the quality of their internal controls, with each meaning something a little different. If an enterprise reported that its controls were "adequate" and if its auditors accepted those assertions in that controls report, the external auditors could be criticized or even face litigation if some significant control problem appeared later.

The Financial Executives International (FEI),[3] a professional organization, got involved in this internal controls reporting controversy. Just as the IIA is the professional enterprise for internal auditors and the AICPA represents public accountants in the United States, the FEI represents enterprise senior financial officers. In the late 1970s, the FEI endorsed the Cohen Commission's internal controls recommendations and agreed that corporations should report on the status of their internal accounting controls. As a result, many U.S. corporations began to discuss the adequacy of internal controls as part of their annual report management letters. These internal control letters were entirely voluntary and did not follow any standard format. They typically included comments stating that management, through its internal auditors, periodically assessed the quality of its internal controls. These "negative assurance" comments indicated that nothing was found to indicate that there might be any internal control problem in operations.

This term *negative assurance* will return in our discussions of internal controls. Because an external auditor cannot detect all problems and faces the risk of potential litigation, pre-SOx external auditor reports often were stated in terms of a negative assurance. That is, rather than saying that they "found no problems" in an area under review, reports would state that the auditors did not find anything that would lead them to believe that there was a problem. This is a subtle but important difference.

Using both the Cohen Commission and the FEI's recommendations, the SEC subsequently issued proposed rules calling for *mandatory* management reports on an entity's internal accounting control system. The SEC stated that information on the effectiveness of an entity's internal control system was necessary to allow investors to better evaluate both management's performance and the integrity of published financial reports. This SEC proposal again raised a storm of controversy; many chief executive officers (CEOs) and chief financial officers (CFOs) felt that this was too onerous, particularly on top of the newly released FCPA regulations.

Questions came from many directions regarding the definition of internal accounting control. While corporations might agree to voluntary reporting, they did

not want to subject themselves—in those pre-SOx days—to the penalties associated with a violation of SEC regulations. The SEC soon dropped the requirement for a separate report on internal accounting controls as part of the annual report to shareholders but promised to rerelease the regulations at a later date.

(a) Earlier AICPA Standards: SAS No. 55

Prior to SOx, the AICPA was responsible for releasing external audit standards through Statements on Auditing Standards (SASs). As discussed for SAS No. 1, these standards formed the basis of the external auditor's review of the adequacy and fairness of published financial statements. Although they underwent a few changes over the years, in the 1970s and 1980s, the AICPA was frequently criticized that its audit standards did not provide adequate guidance to either external auditors or the users of their reports. This problem was called the "expectations gap," because existing public accounting standards did not meet the expectations of investors.

To answer this criticism, the AICPA released a series of new SASs on internal control audit standards between 1980 and 1985. These included SAS No. 30, *Reporting on Internal Accounting Control,* which provided guidance for the terminology to be used in internal accounting control reports. That SAS did not provide much help, however, on defining the underlying concepts of internal control and was viewed by critics of the public accounting profession as too little too late. SAS No. 55, *Consideration of the Internal Control Structure in a Financial Statement Audit*, was another new standard that defined internal control in terms of three key elements:

1. Control environment
2. Accounting system
3. Control procedures

SAS No. 55 presented a different approach to understanding internal controls than had been used in the past, and it has provided a foundation for much of our ongoing understanding of internal controls. Prior to SAS No. 55, an enterprise's internal control structure policies and procedures were often not formally considered by the external auditors. Examples of these internal control processes include policies and procedures concerning the effectiveness, economy, and efficiency of certain management decision-making processes or procedures covering research and development activities. Although certainly important to the enterprise, any related internal control concerns did not ordinarily relate to the external auditor's financial statement audit.

SAS No. 55 defined internal control in a much broader way than was typical for external auditors and provided a basis for the COSO report's definition of the term. SAS No. 55 became effective in 1990 and represented a major stride toward providing external auditors with an appropriate definition of internal control.

(b) Treadway Committee Report

During the late 1970s and early 1980s, many major U.S. enterprises failed due to high inflation and the resultant high interest rates. Many times enterprises reported adequate earnings in their audited financial reports, only to suffer a financial collapse shortly after the release of those reports. A few of these failures were caused by

fraudulent financial reporting, although many others were due to high inflation or other enterprise instability issues. Nevertheless, several members of Congress proposed legislation to "correct" these potential business and audit failures. Bills were drafted, congressional hearings were held, but no legislation was passed.

Also in response to these concerns as well as to the lack of legislative action, the National Commission on Fraudulent Financial Reporting was formed. It consisted of five professional organizations: the IIA, AICPA, and FEI, all mentioned previously, as well as the American Accounting Association (AAA) and the Institute of Management Accountants (IMA). The AAA is a professional organization for the academic accountants. The IMA is the professional organization for managerial or cost accountants.

The National Commission on Fraudulent Financial Reporting came to be called the Treadway Commission after the name of its chairperson. Its major objectives were to identify the causal factors that allowed fraudulent financial reporting and to make recommendations to reduce their incidence. The Treadway Commission's final report was issued in 1987[4] and included recommendations to management, boards of directors, the public accounting profession, and others. It again called for management reports on the effectiveness of internal control systems and emphasized key elements in what it felt should be a system of internal control, including a strong control environment, codes of conduct, a competent and involved audit committee, and a strong internal audit function. The Treadway Commission report again pointed out the lack of a consistent definition of internal control, suggesting further work was needed. The same COSO that managed the Treadway report subsequently contracted with outside specialists and embarked on a new project to define the concept of internal control. Although it issued no standards, the Treadway report was important in raising the level of concern and attention regarding reporting on internal control.

The internal control–reporting efforts discussed here are presented as if they were a series of sequential events. In reality, many of these efforts took place in almost a parallel fashion. This 20-year effort redefined internal control as a basic methodology and outlined a standard terminology for business professionals and auditors. The result has been the COSO internal control framework, discussed in the next sections and referenced throughout this book.

3.4 COSO Internal Control Framework

The five professional auditing and accounting organizations that formed a committee—COSO—then released an internal control report, with the official title *Internal Control–Integrated Framework*.[5] Throughout this book, it is referred to as the COSO internal controls report or framework. These sponsoring organizations contracted with a public accounting firm and used a large number of volunteers to develop the report, releasing a draft in 1990 for public exposure and comment. More than 40,000 copies of the COSO internal controls draft version were sent to corporate officers, internal and external auditors, legislators, academics, and other interested parties with requests for formal comments. Review procedures in the draft, discussed in Section 3.04, were field-tested by major public accounting firms.

After some adjustments, the final COSO internal controls report was released in September 1992. Although not a mandatory standard then, the report proposed a common framework for the definition of internal control as well as procedures

to evaluate those controls. In only a few, the COSO internal controls framework has become the worldwide recognized standard for understanding and establishing effective internal controls in virtually all business systems. The next paragraphs provide a fairly detailed description of the COSO internal controls framework and its use by internal auditors and business professional for internal controls assessments and evaluations.

Virtually every public corporation has a complex control procedures structure. Following the format of a classic organization chart, there may be levels of senior and middle management in multiple operating units or within different activities. In addition, control procedures may be somewhat different at each of these levels and components. For example, one operating unit may operate in a regulated business environment where its control processes are very structured, while another unit may operate almost as an entrepreneurial start-up with a less formal structure. Different levels of management in these enterprises will have different control concern perspectives. The question "How do you describe your system of internal controls?" might receive different answers from persons in different levels or units in each of these enterprise components.

COSO provides an excellent description of this multidimensional concept of internal controls, defining internal control in this way:

> *Internal control is a* process, *affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:*
>
> - *Effectiveness and efficiency of operations*
> - *Reliability of financial reporting*
> - *Compliance with applicable laws and regulations*[6]

Based on this very general definition of internal control, COSO uses a three-dimensional model to describe an internal control system in an enterprise. Exhibit 3.1 presents this COSO internal control framework as a three-dimensional model with five levels on the front-facing side and the three major components of internal control on the top of the diagram—internal controls financial reporting, compliance, and operations—representing the effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. The right-hand side of the exhibit shows segments, but there could be multiples of these depending on the structure of the enterprise.

Each of the COSO internal control framework's levels, from monitoring on top down to the internal controls environment, is discussed in greater detail in the sections to come. The idea here is that when we look at the middle internal control activity layer—such as the period-end financial close—we should consider that control in terms of the business unit or entity or the multiple divisions on the side of the framework where that control has been installed. However, in this three-dimensional model, each control is related to all others in the same row, stack, or column.

The point of the COSO internal controls model or framework is that we must always consider each identified internal control in terms of how it relates to other associated internal controls. As an example of end-of-period financial close internal controls, the enterprise should have information and communication links attached to the financial close processes and the control should be monitored. Dropping down

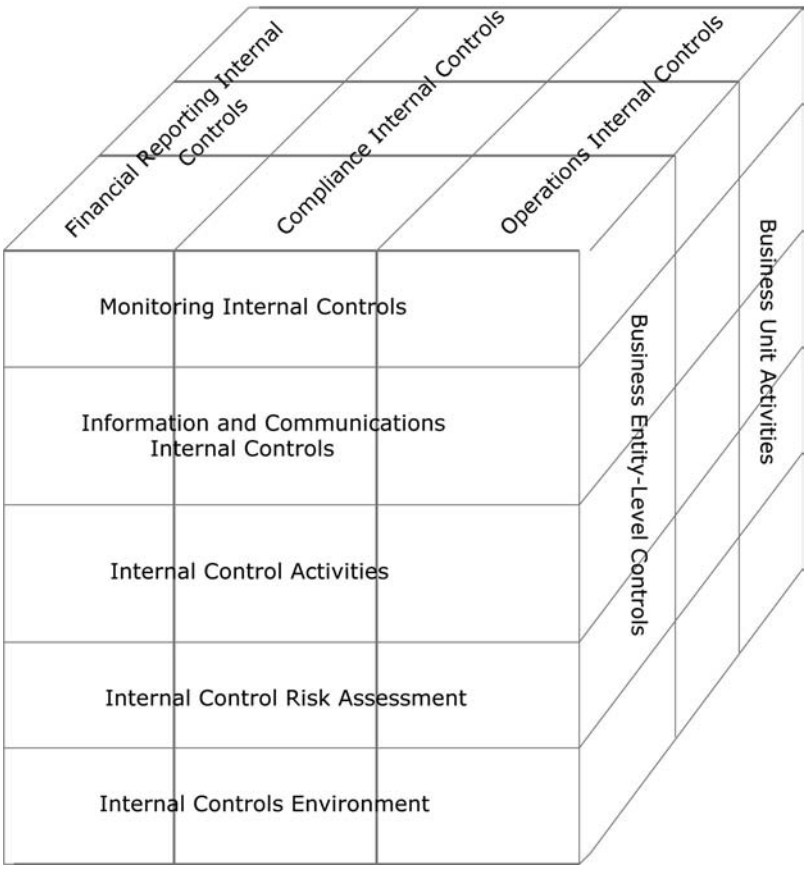


EXHIBIT 3.1 COSO Internal Control Framework

a level, there should be a risk assessment associated with that financial controls process, and it should operate in an appropriate internal controls environment. Compliance and operations issues may also have factors on the specific control that may function at any level in the enterprise organization.

All internal auditors must develop an understanding of this COSO internal controls framework. No matter what area under is review, internal auditors always need to look at internal controls in this multilevel and three-dimensional manner. While this is true for all internal audit work, the concept is particularly valuable when assessing and evaluating internal controls using the COSO internal controls framework. Starting with the first or bottom front-facing level, the following sections describe the COSO internal controls framework elements or components in greater detail:

(a) Control Environment

The foundation of any internal control structure is what COSO calls the *internal control environment*. COSO emphasizes that this internal control environment

foundation entity has a pervasive influence on how all activities are structured and risks assessed. The control environment is a foundation for all other components of internal control; it has an influence on each of the three objectives and on overall unit and entity activities. The control environment reflects the overall attitude, awareness, and actions by the board of directors, management, and others concerning the importance of internal control in the enterprise. While there are many differing fundamental concepts here, each enterprise should have its own unique internal control foundation to support its other internal controls structures.

Enterprise history and culture often play a major role in forming the internal control environment. When an enterprise historically has had a strong management emphasis on producing error-free products, when senior management continues to emphasize the importance of high-quality products, and when this message is communicated to all levels, it becomes a major enterprise control environment factor. For example, messages from the CEO or other very senior managers are known as the tone at the top—management's messages to all stakeholders. However, if senior management has had a reputation of looking the other way from policy violations, this negative message will be communicated to other levels in the enterprise. A positive tone at the top by senior management provides a firm foundation on which to establish the overall control environment for the enterprise.

The next sections outline some of the major elements of the COSO control environment component of internal control. When performing virtually all reviews, internal auditors should always try to understand and evaluate this overall control environment. When the internal control environment is weak, an internal auditor will almost certainly find additional internal control concern areas. In smaller enterprises, the control environment factors will be more informal, but the focus still should be on appropriate control environment factors throughout the entity, as essential components of internal control. The next paragraphs describe the components of the control environment. An enterprise should have implemented elements of each.

(i) **INTEGRITY AND ETHICAL VALUES** The collective integrity and ethical values of an enterprise are essential control environment elements. These values are often defined by the tone-at-the-top messages communicated by senior management. If the enterprise has developed a strong code of conduct that emphasizes integrity and ethical values, and if stakeholders appear to follow that code, all stakeholders will have assurances that the enterprise has a good set of values.

A code of ethics is an important component of organizational governance and is discussed further in Chapter 24. However, even though an enterprise may have a strong code of conduct, many times its principles are violated through ignorance rather than by deliberate malfeasance. In many instances, employees may not know that they are doing something wrong or may believe that their actions are in the enterprise's best interests. This ignorance is often caused by poor senior management moral guidance rather than by any employee intent to deceive, and the enterprise's policies and values must be communicated to all organizational levels. While there can always be bad apples in any enterprise, strong moral messages will encourage everyone to act correctly. The objective should always be to transmit appropriate messages or signals throughout the enterprise.

All stakeholders, and certainly internal auditors, should have a good understanding of their enterprise's code of conduct and how it is applied. If the existing code is outdated, if it does not appear to address important ethical issues facing an

enterprise, or if management does not appear to be communicating the code to all stakeholders on a recurring basis, management needs to wake up and correct this deficiency. If the enterprise does not have a formal ethics office, the initiation of such a function may help in the dissemination of the enterprise's code of conduct.

The code of conduct describes the rules for ethical behavior. Senior management should transmit a proper ethical message throughout the enterprise. Other incentives and temptations, however, can erode this overall control environment. Individuals may be tempted to engage in dishonest, illegal, or unethical acts if their enterprise gives them strong incentives or temptations to do so. For example, an enterprise may establish very high, unrealistic performance targets for sales or production quotas. If there are strong rewards for the achievement of these performance goals—or worse, strong threats for missed targets—employees may be encouraged to engage in fraudulent or questionable practices to achieve those goals. The kinds of temptations that encourage stakeholders to engage in improper accounting or similar acts include:

- Nonexistent or ineffective controls, such as poor segregation of duties arrangements in sensitive areas, that offer temptations to steal or to conceal poor performance
- High decentralization that leaves top management unaware of actions taken at lower enterprise levels and thereby reduces the chances of getting caught
- A weak internal audit function that has neither the ability nor the authority to detect and report improper behavior; this is an area where internal audit can fix itself by performing effective internals audits (see Chapter 7)
- Penalties for improper behavior that are insignificant or unpublicized, causing them to lose their value as deterrents

In order to build integrity and ethical values, a strong internal audit function should be a major component of the COSO control environment. If internal audit finds that management is placing constraints on the audit function, internal audit and its chief audit executive (CAE) should remind management of their importance as part of the enterprise's overall internal control structure and, more important, communicate these concerns to the board of directors audit committee. This important audit committee relationship is discussed in Chapter 23.

(ii) COMMITMENT TO COMPETENCE An enterprise's control environment can be seriously eroded if a significant number of positions are filled with persons lacking required job skills. Internal auditors, in particular, will encounter this situation from time to time in their reviews, interviewing a person assigned to a particular job who does not seem to have the appropriate skills, training, or even intelligence to perform that job. Because all humans have different levels of skills and abilities, adequate supervision and training should be available to help these persons until the staff is upgraded or proper skills are acquired.

An enterprise needs to specify the required competence levels for its various job tasks and to translate those requirements into necessary levels of knowledge and skill. By placing the proper people in appropriate jobs and giving adequate training when required, an enterprise is satisfying this important COSO control environment component.

An assessment of staff competence is an important portion of the control environment, and it can be difficult. How does an internal auditor determine the competence of audit area staff? A strong human resources function, with adequate assessment procedures, is important. However, with regard to assigned work duties, Chapters 7 through 11 should provide some guidance.

(iii) BOARD OF DIRECTORS AND AUDIT COMMITTEE The control environment is very much influenced by the actions of an enterprise's board of directors and its audit committee. In years prior to SOx, boards and their audit committees often were dominated by senior management inside directors, with a limited representation from outside, minority board members. This created situations where the boards were not totally independent of management. Enterprise officers sat on the board and were, in effect, managing themselves, often with less concern for the outside investors. As will be discussed in Chapter 4, SOx has changed this and now requires audit committees to be truly independent. An active and independent board is an essential component of the COSO control environment. By setting high-level policies and by reviewing overall enterprise conduct, the board and its audit committee have the ultimate responsibility for setting this tone at the top. Chapter 23 discusses internal audit's communications with the audit committee.

(iv) MANAGEMENT'S PHILOSOPHY AND OPERATING STYLE The philosophy and operating style of senior management has a considerable influence over an enterprise's control environment. Some top-level managers take significant enterprise-level risks in their new business or product ventures; others are very cautious or conservative. Some managers seem to operate by the seat of their pants while others insist that everything must be properly approved and documented. Some may take very aggressive approaches in their interpretations of tax and financial-reporting rules; others go by the book. These comments do not necessarily mean that one approach is always good and the other bad. A small, entrepreneurial enterprise may be forced to take certain business risks to remain competitive while one in a highly regulated industry would be risk-averse. This concept, called the appetite for risk, is discussed in Chapter 6.

These management philosophy and operational-style considerations are all part of an enterprise's control environment. Internal auditors responsible for assessing internal controls should understand these factors and take them into consideration when evaluating internal controls effectiveness. No one set of styles and philosophies is best for all enterprises, but these factors are important when considering the other components of internal control in an enterprise.

(v) ORGANIZATIONAL STRUCTURE This internal control component provides a framework for planning, executing, controlling, and monitoring activities to help achieve overall objectives. This control environment factor relates to how functions are managed and organized, following a classic organizational chart. Some enterprises are highly centralized; others are decentralized by product, geography, or other factors. Still others are organized in a matrix manner with no single direct line of reporting. Organizational structure is an important aspect of the enterprise's control environment, but no one structure provides any preferred internal controls environment.

An organizational structure is the manner or approach for individual work efforts to be both assigned and integrated for the achievement of overall goals. While this concept could be applied to the manner in which a single individual organizes efforts, it is more applicable to a unit or group effort. For a larger modern enterprise, a strong plan of organization is an important component of its system of internal control. Individuals and subgroups must have an understanding of the total goals and objectives of the group or entity of which they are a part. Without such an understanding, there can be significant internal control weaknesses.

Every enterprise or entity—whether business, government, or not-for-profit—needs an effective plan of organization. Often a weakness in organization controls can have a pervasive effect throughout the total control environment. Despite clear lines of authority, enterprises sometimes have built-in inefficiencies that can become greater as they expand over time, causing control procedures to break down.

(vi) ASSIGNMENT OF AUTHORITY AND RESPONSIBILITY This COSO framework-defined aspect of the control environment is similar to the organizational structure component. An enterprise's organizational structure defines the assignment and integration of its total work effort. The assignment of authority is essentially the way responsibilities are defined in terms of job descriptions and structured in terms of enterprise charts. Although job assignments can never fully escape some overlapping or joint responsibilities, the more precisely these responsibilities can be stated, the better. The failure to clearly define authority and workplace responsibility often causes confusion and conflict between individual and group work efforts.

Today many enterprises of all types and sizes have streamlined their operations and pushed their decision-making authority downward and closer to the front-line personnel. A strong control environment says that front-line employees should have the knowledge and power to make appropriate decisions in their own area of operations rather than be required to pass the request for a decision up through enterprise channels. The critical challenge that goes with this empowerment is that although senior management can delegate some authority in order to achieve objectives, ultimately senior management is responsible for the decisions made by subordinates. An enterprise can place itself at risk if too many decisions involving higher-level objectives are delegated to inappropriate levels without adequate management review. In addition, each person in the enterprise must have a good understanding of the enterprise's overall objectives and how individual actions interrelate to achieve those objectives. The framework section of the COSO internal controls report describes this very important area of the control environment:

> *The control environment is greatly influenced by the extent to which individuals recognize they will be held accountable. This holds true all the way to the chief executive, who has ultimate responsibility for all activities within an entity, including internal control system.*

(vii) HUMAN RESOURCES POLICIES AND PRACTICES Human resource practices cover such areas as hiring, orientation, training, evaluating, counseling, promoting, compensating, and taking appropriate remedial actions. While the human resources function should have adequate published policies and guidance materials, its actual practices send strong messages to employees regarding expected levels of internal controls compliance, ethical behavior, and competence. Higher-level employees

who openly abuse a human resources policy, such as a plant smoking ban, quickly send a message to other levels in the enterprise. The message grows even louder when lower-level employees are disciplined for violating that same smoking ban while higher-level violators are not.

Areas where these human resources policies and practices are particularly important include:

- **Recruitment and hiring.** The enterprise should take steps to hire the best, most qualified candidates. Backgrounds of potential employees should be verified, and interviews should be well organized and in-depth. The interviews also should transmit a message about the enterprise's values, culture, and operating style.
- **New employee orientation.** New employees should be given a clear signal regarding the enterprise's value system and the consequences of not complying with those values. This is the time when new employees are introduced to the code of conduct and asked to formally acknowledge acceptance of that code. Without these messages, new employees may join an enterprise without an appropriate understanding of its values.
- **Evaluation, promotion, and compensation.** There should be a fair performance-evaluation program in place. Because issues such as evaluation and compensation can violate employee confidentiality, the overall system should be established in a manner that is fair all stakeholders in the enterprise.
- **Disciplinary actions.** Consistent and well-understood policies for disciplinary actions should be in place. Employees at all levels should know that if they violate certain rules, they will be subject to a progression of disciplinary actions leading up to dismissal. The enterprise should take care to ensure that no double standard exists for disciplinary actions—or, if any such double standard does exist, that higher-level employees are subject to even more severe disciplinary actions.

Effective human resource policies and procedures are a critical component in the overall control environment. Messages from the top of strong enterprise structures will accomplish little if the enterprise does not have strong human resource policies and procedures in place. Internal audit should always consider this element when performing reviews of other elements of the internal control framework.

(viii) COSO CONTROL ENVIRONMENT IN PERSPECTIVE As somewhat of a different view, Exhibit 3.2 shows the COSO internal control as a pyramid, with the control environment as its foundation. Here, the information and communications component is not shown as an individual layer in the model but a side component that encompasses the Risk Assessment and Control Activities layers. This view was more common when the COSO internal control framework was first drafted, but the Exhibit 3.1 version is much more common today. This view does not really describe the components separated entity by entity shown in the right hand side of Exhibit 3.1.

Although not the typical view of the COSO internal controls framework, this concept is important. Just as a strong foundation is necessary for a multistory building, the control environment provides the foundation for the other components of internal control. An enterprise that is building a strong internal control structure should give special attention to placing solid foundation bricks. Of course, internal auditors

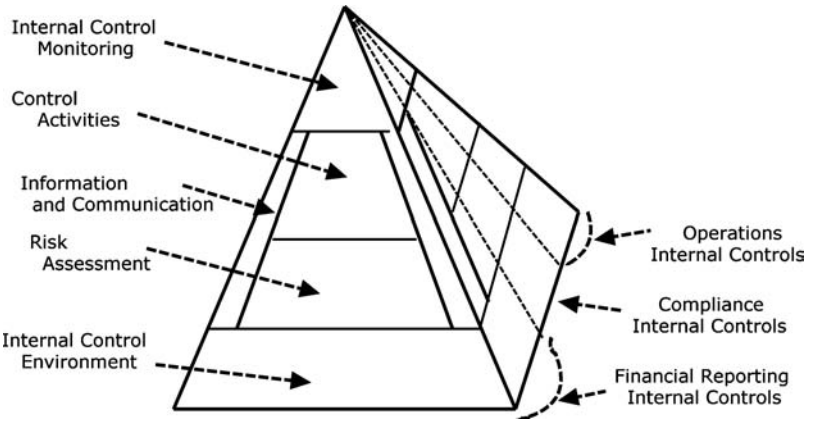


EXHIBIT 3.2 COSO Internal Control Foundation Components

should also keep this concept in mind when assessing internal controls. Internal audit is a key part of this foundation, but the other components are essential as well.

Evaluating the COSO internal control environment does not just require a series of "do the debits equal the credits?" types of rules or measures, but points to the need for strong overall policies that are fundamental but still may be different in many enterprises. For example, there is no set of rules for defining what is meant by tone at the top; each executive's message may be different. However, the CEO and other key managers should adequately communicate these important enterprise messages, usually following the CEO's lead.

(b) Risk Assessment

Exhibit 3.1 shows the next level above the control foundation as risk assessment. An enterprise's ability to achieve its objectives can be at risk due to a variety of internal and external factors. Understanding and management of the risk environment is a basic element of the internal control foundation, and an enterprise should have a process in place to evaluate the potential risks that may impact attainment of its objectives. This risk assessment component focuses on internal controls within an enterprise and has a much narrower focus than the COSO ERM framework discussed in Chapter 6.

COSO internal controls risk assessment should be a forward-looking process that is performed at all levels and for virtually all activities within the enterprise. COSO describes risk assessment as a three-step process:

1. Estimate the significance of the risk.
2. Assess the likelihood or frequency of the risk occurring.
3. Consider how the risk should be managed and assess what actions must be taken.

This COSO risk assessment process places responsibility on management to assess whether a risk is significant and, if so, to take appropriate actions. COSO internal controls also emphasizes that risk analysis is not a theoretical process; often

it is critical to an entity's overall success. As part of its overall assessment of internal control, management should take steps to assess both the risks that may impact the overall enterprise and those pertaining to various enterprise activities or entities. A variety of risks, caused by either internal or external sources, may affect the overall enterprise. The COSO internal controls framework suggests that risks should be considered from three perspectives:

1. **Enterprise risks due to external factors.** These risks include technological developments that can affect the nature and timing of new product research and development or lead to changes in procurement processes. Other external factor risks include changing customer needs or expectations, pricing, warranties, or service activities. New legislation or regulations can force changes in operating policies or strategies, and catastrophes, such as the World Trade Center 9/11 terrorist attack, can lead to changes in operations and highlight the need for contingency planning. These risk factors are very close to elements of the COSO ERM framework discussed in Chapter 6.
2. **Enterprise risks due to internal factors.** As internal auditors often highlight in their ongoing reviews, there can be many types of enterprise-level risks. For example, a disruption in an enterprise's IT server or storage management processing facility can adversely affect overall operations. Also, the quality of personnel hired, as well as their training or motivation, can influence the level of control consciousness within the entity. In addition, the extent of employee accessibility to assets can contribute to misappropriation of resources. Although now better remedied by SOx, the COSO internal controls report also cited the risk of an unassertive or ineffective board or audit committee that can provide opportunities for indiscretions.
3. **Specifi activity-level risks.** Besides being viewed at an enterprise-wide level, risks should also be considered for each significant business unit and key activity, such as for marketing, IT, and finance. These activity-level concerns contribute to the enterprise-wide risks and should be identified on an ongoing basis, considered in the various planning processes throughout the enterprise. Where no such risk-assessment process exists in an enterprise, internal auditors should consider this lack of a formal process as parts of an overall internal controls assessment.

All too often, management may have processes in place that give the appearance of risk assessments but are lacking substance. For example, a new product authorization approval form may include a selection box for the requester to describe the risks associated with the proposed product. Local management may consistently describe them as "low," with no further analysis until there is some type of massive failure. When performing reviews in these areas, internal auditors should review this analysis and discuss the reasoning behind these types of low-risk assessments.

There has been much misunderstanding and confusion regarding the risk assessment element of COSO internal controls because of the similarly named COSO ERM framework. The risk assessment component of the framework includes risk assessments for *within* an individual enterprise. The COSO ERM framework covers the entire entity and beyond. These are two separate issues; one is not a replacement for the other.

(c) Control Activities

The next layer up in the Exhibit 3.1 COSO internal control framework is called control activities. This layer also appears as a separate horizontal layer above Control Activities in Exhibit 3.2, but is encompassed here by the Information and Communication component. Control Activities are the policies and procedures that help ensure that actions identified to address risks are carried out, following a wide range of controls activities sub-processes. Control activities exist at all levels within an enterprise and, in many cases, may overlap one another. The concept of control activities is an essential part of building and then establishing effective internal controls in an enterprise. The COSO internal controls framework identifies a series of these activities by type of process. From an internal audit perspective, they should together be helpful in building effective overall internal controls.

(i) **TYPES OF CONTROL ACTIVITIES** Internal controls are generally classified as manual, IT, or management controls, and they are also described in terms of whether they are preventive, corrective, or detective control activities. While no one set of internal control definitions is correct for all situations, COSO internal controls suggests a way to classify these control activities in an enterprise. Although it certainly is not an all-inclusive list, the next points represent some of these COSO-recommended internal control activities for an enterprise:

- **Top-level reviews.** Management and internal auditors, at various levels, should review the results of their performance, contrasting those results with budgets, competitive statistics, and other benchmark measurements. Management actions to follow up on the results of these top-level reviews and to take corrective action represent a control activity.
- **Direct functional or activity management.** Managers at various levels should review the operational reports from their control systems and take corrective action as appropriate. Many management systems have been built to produce exception reports covering these control activities. For example, an IT security system will have a mechanism to report unauthorized access attempts. The control activity here is the management process of following up on these reported events and taking appropriate corrective action. Some of these activities link very closely with the Information Technology Infrastructure Library (ITIL) best practices discussed in Chapter 18.
- **Information processing.** IT systems contain many controls where systems internally check for compliance in certain areas and then report any internal control exceptions. Those reported exception items should receive corrective action by automated systems procedures, by operational personnel, or by management. Other control activities include controls over the development of new systems or over access to data and program files.
- **Physical controls.** An enterprise should have appropriate control over its physical assets, including fixtures, inventories, and negotiable securities. An active program of periodic physical inventories represents a major control activity here, and internal auditors can play a major role in monitoring compliance.
- **Performance indicators.** Management should relate sets of data, both operational and financial, to one another and take appropriate analytical, investigative,

or corrective actions. This process represents an important enterprise control activity that can also satisfy financial- and operational-reporting requirements.

- **Segregation of duties.** Duties should be segregated among different people to reduce the risk of error or inappropriate actions. This basic internal control procedure should be on almost every internal auditor's radar screen.

These control activities are included in the COSO internal controls report but represent only a small number of the many control activities performed in the normal course of business. These and others keep an enterprise on track toward achieving its many objectives. Control activities usually involve both a policy establishing what should be done and procedures to effect those policies. While these internal control activities sometimes may be communicated only orally, according to COSO internal controls, no matter how they are communicated, the matter should be implemented "thoughtfully, conscientiously, and consistently." This is a strong message for internal auditors reviewing internal control activities. Even though an enterprise may have a published policy covering a given area, there should be established internal control procedures to support that policy. Procedures are of little use unless there is a sharp focus on the condition to which they are directed. All too often, an enterprise may establish a control violations exception report, as part of an IT system, yet reported control violations receive little more than a cursory review by the report recipients. However, depending on the types of conditions reported, those exceptions should receive appropriate follow-up actions.

(ii) INTEGRATION OF CONTROL ACTIVITIES WITH RISK ASSESSMENT Control activities should be closely related to the identified risks from the COSO internal controls risk assessment component. Internal control is a process, and appropriate control activities should be installed to address identified risks. Control activities should not be installed just because they seem to be the right thing to do even if there are no significant risks in the area where the control activity would be installed. Sometimes control activities in place once served some control-risk concern, although the concerns have largely gone away. A control activity or procedure should not be discarded just because there have not been control violation incidents in recent years, but management needs periodically to reevaluate the relative risks. All internal control activities should contribute to the overall control structure. Internal auditors should keep this concept in mind as they review internal controls and make recommendations.

(iii) CONTROLS OVER INFORMATION SYSTEMS The COSO internal controls framework emphasizes that control procedures are needed over all significant IT or information systems—financial, operational, and compliance related. COSO internal controls breaks down information systems controls into the well-recognized general and application controls. General controls apply to much of the function of the information systems to help ensure adequate control procedures over all applications. A physical security lock on the door to the IT server center is such a general control for all applications running in on servers within that facility. Compliance with Chapter 18's ITIL best practices will help top ensure strong IT general controls.

The term *application controls* refers to specific IT processes. A control in a weekly payroll IT program that prevents any employee from being paid for over 80 hours in a given week is an example of an application reasonableness control.

People may work extra hours, but it is doubtful many will record over 80 hours in a week. The COSO internal controls framework highlights a series of IT control areas for evaluating the overall adequacy of internal controls. General controls include all centralized server center or data storage management controls, including job scheduling, database management, and business continuity planning. These controls typically are the responsibility of specialists in centralized computer server or storage management centers. However, with newer, more modern systems connected to one another through telecommunications and network links, these controls can be distributed across a large web of server-based systems.

The COSO internal controls framework document concludes with a discussion on the need to consider the impact of evolving technologies when evaluating information systems control activities. Due to the rapid introduction of new technologies, what is new today will soon be replaced by something else. COSO internal controls have not introduced anything new with regard to IT controls but highlighted their importance in the overall internal control environment.

(d) Communications and Information

Exhibit 3.1, the model of the COSO internal controls framework, describes its components as layers, one on top of another, starting with the Internal Controls Environment as the foundation. The pyramid model in Exhibit 3.2 describes the information and communication component not as a horizontal layer but a side element that crosses other components. Information and communications are related but distinct components of the internal control framework. Appropriate information, supported by IT systems, must be communicated up and down the enterprise in a manner and time that allows people to carry out their responsibilities. In addition to formal and informal communication systems, enterprises must have effective procedures in place to communicate with internal and external parties. These information and communication flows in the enterprise must be understood for any internal control evaluation, such as for a SOx Section 404 evaluation.

(i) RELATIONSHIP OF INFORMATION AND INTERNAL CONTROL An enterprise needs information at all levels to achieve its operational, financial, and compliance objectives. For example, the enterprise needs information to prepare financial reports that are communicated to outside investors as well as internal cost and external market preference information to make correct marketing decisions. This information must flow both from the top levels of the enterprise to lower levels and from the lower levels to the upper levels. COSO internal control takes a broad approach to the concept of an information system, recognizing that systems can be manual, automated, or conceptual. Any of these systems can be formal or informal. Regular conversations with customers or suppliers can be highly important sources of information and are an informal type of an information system. The effective enterprise should have information systems in place to listen to customer requests or complaints and to forward customer-initiated information to appropriate personnel.

COSO IT systems internal controls should emphasize the importance of keeping information and supporting systems consistent with overall enterprise needs. Effective information systems adapt to support changes on many levels. However, internal auditors often encounter cases where an IT application was implemented years ago to support a different set of needs. Although its controls may be good, the

application may not support the enterprise's current needs. COSO internal controls take a broad view of these types of situations and point to the need to understand the current requirements of both manual processes and automated technologies.

Strategic and Integrated Systems Accounting and financial processes were the first enterprise automated or IT systems, starting with the unit record or IBM card accounting machines in the 1950s and then moving to the earliest computer systems. Most enterprises today have upgraded their IT systems many, many times, but sometimes their basic mix of supporting processes may not have changed significantly. An enterprise will have its general ledger, payroll, inventory, accounts receivable, accounts payable, and related core information systems, without too much else. COSO internal control suggests that the effective enterprise should go beyond these core applications to implement strategic and integrated information systems.

By a *strategic system*, the COSO internal control report suggests that management should consider the planning, design, and implementation of its information systems as part of its overall enterprise strategy. These strategic systems then support the enterprise's business and help it to carry out its overall business missions. Many enterprises developed strategic information systems to support their business strategies—systems that allowed them to respond better to changes in their marketplaces and control environments.

COSO internal control also emphasizes the importance of integrating automated information systems with other operations. Examples would be a fully automated manufacturing system that controls both production machines and equipment inventories or a highly automated distribution system that controls inventory and schedules shipments. COSO internal control makes the point, however, that just because a system is new, it will not necessarily provide better controls. Older applications have been tried and tested through use; new systems can have unknown or untested control weaknesses.

Quality of Information The COSO internal controls report has a brief section on the importance of the quality of information. Poor-quality information systems, filled with errors and omissions, affect management's ability to make appropriate decisions. Reports should contain enough data and information to support effective internal control activities. To determine the quality of information, one must ascertain whether:

- The content of reported information is appropriate.
- The information is timely and available when required.
- The information is current or at least the latest available.
- The data and information are correct.
- The information is accessible to appropriate parties.

These points all circle back to many internal audit control concerns and to SOx Section 404 requirements outlined in Chapter 4. While the COSO framework holds up quality of information as an internal controls objective, SOx effectively makes the need for quality a requirement. Beyond classic internal audit and controls concerns, attention should be on the quality of the information produced by all manual and automated systems (discussed in Chapter 31).

(ii) THE COMMUNICATIONS ASPECT OF INTERNAL CONTROL Communications is defined as a separate internal control element in COSO's internal control framework. Communication channels allow individuals to carry out their financial reporting, operational, and compliance responsibilities. COSO emphasizes that communication must take place on a broad level, including dealing with individuals or groups and with their expectations. Appropriate channels of communication are an important element in the overall framework of internal control, and an enterprise needs to establish these channels throughout its various organizational levels and activities as well as with interested outsiders. Although communication channels can have many dimensions, COSO internal control highlights the separate components of internal and external communications. Internal auditors have always focused on formal channels of communication, such as IT applications, procedure manuals, or published documentation. While that documentation is a very important element of communication, COSO takes an expanded view here when considering internal control.

Communications: Internal Components According to COSO internal control, perhaps the most important component of the communications element is that stakeholders should receive messages from senior management reminding them of their internal control responsibilities. The clarity of this message is important to ensure that the enterprise will follow effective internal control principles. This message is part of the tone at the top, discussed as part of the control environment. In addition to these overall messages, all stakeholders need to understand how their specific duties and actions fit into the total internal control system. If this understanding is not present, some may make risky or even bad decisions.

All stakeholders need to know limits and boundaries and when their actions may be unethical, illegal, or otherwise improper. People also need to know how to respond to errors or other unexpected events in the course of performing their duties, and they typically require messages from management, procedure documentation, and adequate training. Internal auditors often encounter situations where an enterprise does not appropriately document such internal control challenges in the course of their reviews. While auditors historically have commented on a lack of documentation, sometimes treating it as a fairly minor point, both COSO internal controls and SOx emphasize that a lack of documentation may mean poor internal control communication channels.

Communication must flow in two directions, and COSO internal control emphasizes that stakeholders must also have a mechanism to report upward throughout the enterprise. This upward communication has two components: communication through both normal and through special, confidential reporting channels. *Normal reporting* refers to the process in which stakeholders are expected to report on status, errors, or problems up through their supervisors. This communication should be freely encouraged, and the enterprise should avoid "shooting the messenger" when bad news is reported. Otherwise, stakeholders will tend to report only good news, and managers may not become aware of significant problems. Because personnel sometimes are reluctant to report matters to their immediate supervisors, whistleblower programs are essential. These are mechanisms by which persons can anonymously report concerns to a higher level in the enterprise for resolution. SOx requires that an audit committee establish a whistleblower program to allow the reporting of internal control errors or improper acts. The current status of SOx whistleblower rules and internal audit's potential role is discussed in Chapter 24.

This section of the COSO internal controls framework concludes with a discussion on the importance of communication channels between top management and the board of directors. Although the COSO internal controls framework now has been in place for over 30 years, its guidelines regarding management informing the board of major developments, risks, and occurrences did not receive sufficient attention until SOx was enacted.

External Communications Enterprises need to establish communication channels with outside parties, including customers, suppliers, shareholders, bankers, regulators, and others. This communication should go beyond the public relations–type of function that large enterprises often establish to talk about themselves. Like internal communication channels, external information must flow in two directions. The information provided to outside parties should be relevant to the needs of those parties, building a better understanding of an enterprise and the challenges it faces. Sending out highly optimistic reports to outsiders when many inside the enterprise realize there are problems also gives an inappropriate internal message.

External communications can be a very important way to identify potential control problems. Customer complaints regarding service, billings, or product quality often point out significant operating and control problems. Independent mechanisms should be established to receive these messages and act on them, including taking corrective action when necessary. Open and frank two-way communications may alert the enterprise to potential communication problems or allow it to discuss and solve any problems in advance of adverse publicity.

Means and Methods of Communication There is no one correct means of communicating internal control information within the enterprise. The modern enterprise can communicate its messages through bulletin board announcements, procedure manuals, Webcasts, videotaped presentation, or speeches by members of management. However, actions taken either before or after the message will give a stronger signal to communication recipients. COSO internal controls summarize this communication element:

> *An entity with a long and rich history of operating with integrity, and whose culture is well understood by people through the enterprise, will likely find little difficulty in communicating its message. An entity without such a tradition will likely need to put more into the way the messages are communicated.*

(e) Monitoring

Exhibit 3.2's pyramid view of COSO internal controls shows Monitoring as the capstone and the upper level of COSO internal control components. While internal control systems will work effectively with proper support from management, control procedures, and information and communication linkages, processes must be in place to monitor these activities. Monitoring has long been the role of internal auditors, who perform reviews to assess compliance with established procedures; however, COSO now takes a broader view of monitoring. COSO internal control recognizes that control procedures and other systems change over time. What appeared to be effective when it was first installed may not be effective in the future.

A monitoring process should be in place to assess the effectiveness of established internal control components and to take corrective action when appropriate. While such a monitoring process certainly points to the important role of internal audit, this internal control component cannot be relegated just to the internal auditors when management remains oblivious to other potential control problems. An enterprise needs to establish a variety of monitoring activities to measure the effectiveness of its internal controls. It can do this through separate evaluations as well as with ongoing activities to monitor performance and take corrective action when required.

(i) **ONGOING MONITOR ACTIVITIES** Many routine business functions can be characterized as monitoring activities. Although internal auditors often do not always think of the functions in that way, COSO internal control gives these examples of the ongoing monitoring component of internal control:

- **Operating management normal functions.** Normal management reviews over operations and financial reports constitute an important ongoing monitoring activity. However, special attention should be given to reported exceptions and potential internal control deviations. Internal control is enhanced if reports are reviewed on a regular basis and corrective action initiated for any reported exceptions.
- **Communications from external parties.** This element of monitoring is closely related to the component of communication from external parties discussed earlier. External communication measuring monitors, such as a customer complaint telephone number, are important; however, the enterprise needs to monitor closely these calls and then initiate corrective action when appropriate.
- **Enterprise structure and supervisory activities.** While senior management should always review summary reports and take corrective actions, the first level of supervision and the related enterprise structure often plays an even more significant role in monitoring. Direct supervision of clerical activities, for example, should routinely review and correct lower-level errors and assure improved clerical employee performance. This is also an area in which COSO emphasizes the importance of an adequate separation of duties. Dividing duties between employees allows them to serve as a monitoring check on one another.
- **Physical inventories and asset reconciliation.** Periodic physical inventories, whether of storeroom stock, negotiable securities, or other assets, are an important monitoring activity. An annual inventory in a retail store, for example, may indicate a significant merchandise loss. Suspected theft could be a possible reason for this loss, pointing to the need for better security controls.

These are just a few examples from the COSO internal controls report. They illustrate procedures that are often in place but are not thought of as ongoing monitoring activities. Any function or process that reviews enterprise activities on a regular basis and then suggests potential corrective actions can be thought of as a monitoring activity.

(ii) **SEPARATE INTERNAL CONTROL EVALUATION** While COSO internal control points out the importance of ongoing monitoring activities to support the internal control framework, it also suggests that "it may be useful to take a fresh look from time to time" at the effectiveness of internal controls through separate evaluations. The

frequency and nature of these separate reviews depends to a large extent on the nature of the enterprise and the significance of the risks it must control. Management may want to initiate an evaluation of its entire internal controls environment periodically, but internal audit should initiate many such reviews to assess specific control areas. These reviews are often initiated when there has been an acquisition, a change in business, or some other significant activity.

COSO also emphasizes that these evaluations may be performed by direct line management through self-assessment reviews. Internal audit is not required to perform these reviews unless requested, and considerable time may pass before internal audit may schedule a normal review in some area of operation. However, responsible management should consider scheduling and performing its own self-assessments on a more regular basis. The internally generated review can point out potential control problems and cause operating management to implement corrective action activities. Because these self-assessment reviews typically are not as comprehensive as a normal internal audit, a follow-up review by internal auditors or others can be launched if potentially significant problems are encountered during a limited self-assessment review.

Internal Control Evaluation Process The COSO internal controls guidance materials outline an evaluation process for reviewing internal controls. The evaluator should: (1) develop an understanding of the system design, (2) test key controls, and (3) develop conclusions based on the test results. This is really the internal audit process. COSO internal control also mentions *benchmarking* as an alternative approach. Benchmarking is the process of comparing an enterprise's processes and control procedures with those of peer enterprises. Comparisons are made with similar enterprises or against published industry statistics. This approach is convenient for some measures but filled with dangers for others. For example, it is fairly easy to benchmark the size, staffing levels, and average compensations of a sales function against comparable enterprises in the same general industry; however, the evaluator may encounter difficulties in trying to compare other factors due to the many small differences that make all enterprises unique. The internal audit process of control self-assessments, discussed in Chapter 11, provides guidance here.

Evaluation Action Plans COSO internal control recognizes that many highly effective procedures are informal and undocumented. Many of these undocumented controls, however, can be tested and evaluated in the same manner as documented ones. While an appropriate level of documentation makes any evaluation of internal control more efficient and facilitates employees' understanding of how the process works, that documentation is not always essential. Internal auditors reviewing an enterprise's internal financial controls systems will certainly request to see some level of systems documentation as part of their review work. If an existing process is informal, undocumented, but recognized as effective, the review team will need to prepare its own evaluation documentation to explain how the process works and the nature of its internal controls.

(iii) REPORTING INTERNAL CONTROL DEFICIENCIES Whether internal control deficiencies are identified through processes in the internal control system itself, through monitoring activities, or through other external events, they should be reported to appropriate levels of enterprise management. The key question for the internal audit

evaluator is to determine what should be reported, given the large number of details that may be encountered, and to whom the reports should be directed. COSO internal control states that "all internal control deficiencies that can affect the entity's attaining its objectives should be reported to those who can take necessary action." While this statement makes sense, it is often difficult to implement. The modern enterprise, no matter how well organized, will be guilty of a variety of internal control errors or omissions. COSO internal control suggests that all of these should be identified and reported and that even the most minor of errors should be investigated to understand if they were caused by any overall control deficiencies. The COSO internal controls report uses the example of an employee's taking a few dollars from the petty cash fund. This could be viewed as a minor matter due to the small amount of the theft, but it still should viewed as a control breakdown on several levels.

While the monetary amount may not be significant, COSO internal control urges that the matter be investigated rather than ignored, since "such apparent condoning personal use of the entity's money might send an unintended message to employees." Prior to SOx, external auditors regularly applied the concept of materiality when performing their reviews. That is, they often decided that some errors and irregularities were so small that they are not material to the external auditor's overall conclusion. In the first years of Section 404 assessments and following the original AS2 auditing standards, the message from many external auditors was that materiality should not be considered—an error is an error. This approach frustrated many managers who wondered why their external auditors were raising issues with what they felt were minor matters. With the AS5 rules discussed in Chapter 4, materiality as well as relative risk should now be considered when evaluating the efficiency and effectiveness of internal controls.

The COSO internal controls guidance concludes by discussing to whom internal control deficiencies in the enterprise should be reported. In one paragraph, COSO internal control provides guidance that is useful for evaluations:

> *Findings on internal control deficiencies usually should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the enterprise whose activities may be affected. Where findings cut across organizational boundaries, the reporting should cross over as well and be directed to a sufficiently high level to ensure appropriate action.*

Internal auditors should be aware the SOx rules have tightened up this COSO internal controls reporting guidance. Matters that appear to be of a material nature become an almost immediate CFO and audit committee reporting issue. The enterprise should also develop reporting procedures such that all internal financial control deficiencies, whether encountered through a SOx Section 404 review or an internal audit review of ongoing operations, are reported to appropriate levels of the enterprise. Management reporting and monitoring is a highly important aspect of internal control. Internal audit has a lead role in that process through internal audit reviews and should be aware of the need for other monitoring processes when reviewing and evaluating internal controls.

3.5 Other Dimensions of the COSO Internal Controls Framework

We sometimes forget that the COSO internal controls framework is a three-dimensional model, as shown in Exhibit 3.1. In addition to the front-facing dimension on the model covering control activities, the right-side dimension covers entities or activities while the top of the framework cube covers the three dimensions of all internal controls:

- Reliability of financial reporting
- Compliance with applicable laws and regulations
- Effectiveness and efficiency of operations

Each of the control areas just discussed—from the control environment to monitoring—should be considered with respect to COSO's other two dimensions.

With consideration given to the right-side dimension, internal controls should be installed and evaluated across all units in the enterprise. This does not mean that a control activity, such as an expense approval process, must be identical in all organizational units, whether at corporate headquarters or a sales office in a remote geographic location. However, there should be a consistent set of control processes throughout the enterprise with consideration given to the relative risks and scope of operations. Internal controls should be consistent, but they should be applied appropriately in individual operating units.

The third or top dimension of the COSO internal controls framework is even more significant. It says that internal control activities should be installed in all operating units and should include the three factors of internal controls: effectiveness, financial reporting reliability, and regulatory compliance. Looking at internal controls from this three-dimensional viewpoint, there may be some variations, but there is a basic and consistent internal controls framework. Consider a subsidiary facility in a West African state, far away from U.S. headquarters. Country expense approval procedures may be subject to local laws, and other processes may be somewhat different due to communication distances or differences in local IT systems. However, those internal controls still should be implemented in a manner that ensures reliability in financial reporting as results are reported up to corporate headquarters.

No matter where they are installed in an enterprise, all COSO internal controls should be considered in terms of the COSO three-dimensional cube. That is, the control must be considered in terms of where it fits in the overall enterprise and its relationship to the three control objective areas. When this is done, internal auditors have a powerful way of looking at internal controls from a total and certainly a SOx perspective. The COSO internal controls framework continues to be an important standard and set of guidance materials for measuring and evaluating internal controls.

The COSO internal controls framework, as shown in Exhibit 3.1, is becoming the worldwide standard for building and developing effective internal controls. It is a continuous process in each of its three dimensions. On the front-facing side of the model, the monitoring component on top is of little value unless internal control processes are in place all the way down the internal control environment foundation. Similarly, effective internal controls must be installed in all levels of organizational units, and each of those controls must be sensitive to the three top-facing internal control elements.

3.6 Internal Audit CBOK Needs

Beginning with this chapter, each chapter will conclude with a brief description of how its contents should be part of most internal auditors' CBOK.

COSO internal control is different from an internal audit CBOK perspective. This framework is becoming the worldwide standard for building and evaluating all levels of internal controls. All internal auditors should understand this three-dimensional approach to looking at and evaluating internal controls. This chapter has summarized the COSO report, *Internal Control–Integrated Framework*, the official description of the COSO internal controls framework. A more detailed study of that report can help internal auditors gain more knowledge about COSO internal controls, an internal audit CBOK essential.

Notes

1. Institute of Internal Auditors, *International Professional Standards for the Practice of Internal Auditing,* Section *2120—Control* (Altamonte Springs, FL: Author, ND). See www.theiia.org.
2. AICPA, *Statement on Auditing Standards No. 1, Codification of Auditing Standards and Procedures, Professional Standards.* www.aicpa.org.
3. Financial Executives International was formerly known as the Financial Executives Institute.
4. National Commission on Fraudulent Financial Reporting, Report, 1987.
5. *Internal Control—Integrated Framework,* www.coso.org/ Note: This reference is for the COSO internal controls report that can be ordered through the AICPA at www.cpa2biz.com.
6. AICPA-published COSO internal control standards are described in these Statements on Auditing Standards: numbers 103, 105, 106, 107, 109, 110, and 112. www.aicpa.org.

CHAPTER 4

Sarbanes-Oxley and Beyond

The Sarbanes-Oxley Act (SOx) is a U.S. law enacted in 2002 to improve financial reporting audit processes and to mandate new board of director, public accounting, and other enterprise governance practices. It has had a major impact on businesses first in the United States and now worldwide. While SOx's new auditing and internal control rules have particularly changed many external auditor practices, SOx also has had a major impact on internal auditors. A general understanding of SOx, with an emphasis on its Section 404 internal accounting control rules, should be a key common body of knowledge (CBOK) requirement for all internal auditors.

SOx became a law in the United States as a response to a series of accounting misdeeds and financial failures at several once-major corporations such as Enron and WorldCom. A major component of SOx is the Public Company Accounting Oversight Board (PCAOB), an independent entity that now sets U.S. external auditing standards and regulates the public accounting industry. SOx is a wide-ranging set of requirements that has redefined how we both govern public enterprises and attest that their reported financial results are fairly stated.

Although SOx is a comprehensive set of legislation with many components, most of the business and auditor attention to SOx requirements has focused on its Section 404 internal control attestation rules. Internal auditors should be particularly aware of the requirements for SOx Section 404 reviews as well as what are called the Section 302 rules, which make management responsible for its reported financial statements. Both of these sections have caused a major amount of effort and concern as corporations began to establish SOx compliance. Other portions of the legislation have not received as much attention or caused major compliance concerns. An example is a SOx requirement that audit committees establish what are called whistleblower programs to report fraudulent accounting anonymously. Although this first appeared to be a significant requirement, it has not received that much attention or activity to date.

This chapter provides an overview of SOx today, with an emphasis on Section 404 and other areas that are most important to internal auditors. An understanding of SOx should be part of an internal auditor's CBOK, and this chapter focuses on three important aspects of SOx:

1. **Key SOx elements: Overview of the legislation.** We summarize SOx rules in such areas as audit committee procedures and new external auditor rules. This overview should help internal auditors to better understand some of these SOx rules.

2. **Section 404 internal accounting control reviews.** The SOx requirements for reviews of internal accounting controls have caused much toil and turmoil in corporations. We describe the review process and why it is important for internal auditors.
3. **SOx's Auditing Standard No. 5 (AS 5) risk-based approaches.** A relatively new set of PCAOB auditing standards called AS 5, these rules call for a more risk-based auditing approach. More important here, AS 5 emphasizes the importance of internal audit's work in performing financial reporting internal control reviews.

Much of the impact of SOx depends on detailed rules released by the PCAOB to interpret the legislation. SOx legislation was drafted in a one-size-fits-all manner, suggesting that SOx and the Securities and Exchange Commission (SEC) rules applied to any entity, despite its size or home country, that has a security registered with the SEC. Those practices are changing. We also look at how SOx is evolving into a worldwide global standard.

4.1 Key Sarbanes-Oxley Act Elements

The official name of SOx is the Public Accounting Reform and Investor Protection Act. It became law in August 2002. Most of the final detailed rules and regulations were released by the end of 2003. As its title is long, business professionals refer to it as the Sarbanes-Oxley Act, from the names of its principal congressional sponsors. Still too long of a name, most generally refer to it as SOx, SOX, or Sarbox, among many other variations.

SOx introduced a series of totally changed processes for external auditing and gave new governance responsibilities to senior executives and board members. SOx also established the PCAOB, a rule-setting authority under the SEC that issues financial auditing standards and monitors external auditor governance. As happens with all financial- and securities-related federal laws, an extensive set of specific regulations and administrative rules has been developed by the SEC based on the SOx legislation.

U.S. federal laws are organized and issued as separate sections of legislation called titles, with numbered sections and subsections under each. Much of the SOx legislation contains rules that are not that significant for most internal auditors and business professionals. For example, Section 602 (d) of Title I states that the SEC "shall establish" minimum professional conduct standards or rules for SEC practicing attorneys. While perhaps good to know, this does not have any internal audit impact. Exhibit 4.1 summarizes the major titles of SOx, and the sections to come describe key SOx titles. Our intent is not to reproduce the full text of this legislation—it can be found on the Web[1] —but to highlight portions of the law that are more significant to internal audit and business professionals. Of interest, even though internal control processes very much rely on both external and internal auditors, the original SOx legislation makes almost no direct references to the important roles and responsibilities of internal auditors. The importance of internal audit in SOx internal control reviews was highlighted subsequently in the AS 5 rules, released in mid-2007 and discussed later. The emphasis throughout this chapter is on the role of internal audit in today's SOx environment.

EXHIBIT 4.1 Sarbanes-Oxley Act Key Provisions Summary

Section	Subject	Rule or Requirement
101	Establishment of PCAOB	Overall rules for the establishment of the PCAOB, including its membership requirements.
104	Accounting Firm Inspections	Schedule for PCAOB inspections of registered public accounting firms.
108	Auditing Standards	The PCAOB will accept current but will issue its own new auditing standards.
201	Out-of-Scope Practices	Outlines prohibited accounting firm practices such as internal audit outsourcing, bookkeeping, and financial systems design.
203	Audit Partner Rotations	The audit partner and the reviewing partner must rotate off an assignment every 5 years.
301	Audit Committee Independence	All audit committee members must be independent directors.
302	Corporate Responsibility for Financial Reports	The CEO and CFO must personally certify their periodic financial reports.
305	Officer and Director Bars	If compensation is received as part of fraudulent/illegal accounting, the benefiting officers or director is required to personally reimburse funds received.
404	Internal Control Reports	Management is responsible for an annual assessment of internal controls.
407	Financial Expert	One audit committee director must be a designated financial expert.
408	Enhanced Review of Financial Disclosures	The SEC may schedule extended reviews of reported information based on certain specified factors.
409	Real-Time Disclosure	Financial reports must be distributed in a rapid and current manner.
1105	Officer or Director Prohibitions	The SEC may prohibit an officer or director form serving in another public company if guilty of a violation.

(a) Title I: Public Company Accounting Oversight Board

The SOx legislation starts with significant new rules for external auditors. Prior to SOx, the American Institute of Certified Public Accountants (AICPA) had the guidance-setting responsibility for all external auditors and their public accounting firms through its administration of the Certified Public Accountant (CPA) test and its restriction of AICPA membership to CPAs. While state boards of accountancy actually licensed CPAs, the AICPA had overall responsibility for the profession. External audit standards were set by the AICPA's Auditing Standards Board (ASB). Although basic standards—called generally accepted auditing standards (GAAS)—have been

in place over the years, newer standards were released as numbered auditing standards called Statements of Auditing Standards (SASs). Much of GAAS was just good auditing practices, such as that accounting transactions must be backed by appropriate documentation. The SASs covered specific areas requiring better definition. SAS No. 79, for example, defined internal control standards, and SAS No. 99 covered the consideration of fraud in a financial statement audit. The AICPA's code of professional conduct requires CPAs to follow and comply with all applicable auditing standards.

The AICPA's GAAS and its numbered SAS standards had been accepted by the SEC, and these auditing rules defined auditing standards and the tests necessary for a certified audited financial statement. However, the accounting scandals that led to the passage of SOx signaled that the AICPA-led process of establishing auditing standards was broken; SOx removed this audit standards-setting process from the AICPA, which was dominated by major public accounting firms, and created the PCAOB, a nonfederal, nonprofit corporation with the responsibility to oversee all audits of corporations subject to the SEC.

The PCAOB does not replace the AICPA but assumes responsibility for the external auditing practices that were formerly managed by AICPA members. The AICPA continues to administer the CPA examination, with its certificates awarded on a state-by-state basis, and sets auditing standards for U.S. private, non-SEC organizations. SOx Title I defines PCAOB auditing practices for external auditors. Other audit process and corporate governance rules have changed how internal auditors coordinate their work with external auditors. The PCAOB also releases rules from time to time to support the basic SOx legislation. As this book goes to press, there have been five standards up through the very important AS 5, discussed in Section 4.3 (see www.pcaobus.org).

The next paragraphs provide some background on SOx Title 1 external audit process rules and the origins of SOx. An understanding of these SOx rules will help internal auditors in their dealings with their external auditors and business management.

(i) PCAOB ADMINISTRATION AND PUBLIC ACCOUNTING FIRM REGISTRATION The PCAOB is administered through a board of five members appointed by the SEC with three members *required* to be public, non-CPA members. SOx requires that the PCAOB is not dominated by CPA and public accounting firm interests, and its chairperson must not have been a practicing CPA for at least the past five years. The PCAOB is responsible for overseeing and regulating all public accounting firms that practice before the SEC, including:

- **Registration of the public accounting firm that perform audits of corporations.** Much more detailed than just filling out an application form and beginning audits, a registering external audit firm must disclose the audit fees collected, describe its audit and quality standards, provide detailed information on its CPAs performing audits, and disclose any pending criminal, civil, or administrative actions. A firm can be denied the right to register due to any PCAOB questions regarding its background.
- **Establish auditing standards.** These standards include auditing, quality control, ethics, independence, and other key audit areas. Although many continue to follow earlier AICPA standards, new PCAOB standards are gradually being

released. Perhaps the most significant to date has been the Auditing Standard No. 5 (AS 5). As there are frequent calls for more continuous auditing and health and safety sustainability reporting audits, we can expect a whole different dimension or approach to auditing standards in the future.

- **Conduct inspections of registered public accounting firms** The AICPA had a peer review process in the past, but often public accounting firms had little criticism of their peers. The PCAOB now performs the quality-related reviews of registered firms.
- **Conduct investigations and disciplinary procedures.** Wrongdoing discovered in formal investigations, whether by an individual auditor or an entire registered firm, can result in sanctions that would prohibit an auditor or a firm from performing audits under PCAOB.
- **Perform other standards and quality functions as the board determines.** The PCAOB has indicated that it may get involved in other areas to protect investors and the public interest. There has been little activity here, but as the need for auditing services evolves, these standards may certainly change and evolve.
- **Enforce SOx compliance.** The PCAOB is responsible for enforcing compliance to SEC auditing rules beyond the SOx legislation. This may result in a variety of administrative law actions or other procedures as appropriate.

Information and results on this public accounting firm registration process can be found at www.pcaob.gov. This published registration data may be of particular value for an enterprise that is not using one of the major public accounting firms. Many medium-size and smaller highly credible public accounting firms can provide an enterprise with excellent, high-quality service, but it is always prudent to check these PCAOB registration records.

(ii) AUDITING, QUALITY CONTROL, AND INDEPENDENCE STANDARDS Title I, Section 103, gives the PCAOB authority to establish auditing and related attestation standards, quality control standards, and ethics standards for registered public accounting firms. SOx accepted the previously issued AICPA auditing standards and states that new auditing standards may be based on "proposals from one or more professional groups of accountants or advisory groups." As we move to a greater global economy and as SOx becomes more of a worldwide standard, we can expect to see international auditing standards, as discussed in Chapter 33, to have an increasing influence.

The Institute of Internal Auditors' (IIA's) *International Standards for the Professional Practice of Internal Auditing,* discussed in Chapter 8, falls into the PCAOB's "standards by other professional groups" category as well. IIA standards are designed to support all internal auditor review work but are not for an external auditor's audit and attest work. When an internal auditor works in support of external audit counterparts on some audit task, this work should follow PCAOB audit guidelines. PCAOB standards cover these areas:

- **Audit workpapers retention** . The PCAOB Standard AS 3, *Audit Documentation,* mandates that audit workpapers and other supporting materials should be maintained for a period of not less than seven years. This requirement is in response to an infamous event concerning Enron and its auditor, Arthur Andersen. Enron was still in operation but was under some financial pressures when the

SEC announced that it were going to conduct an onsite investigation. Enron's external auditors, Arthur Andersen, used an internal firm policy to justify destruction of all but the most current Enron audit documentation. This was a motivating factor that led to this SOx rule.

- **Concurring partner approval.** While external audit standards had required a concurring or second-party approval for each audit report issued, these were often done more for an after-the-fact quality control review. Under SOx rules, a second external audit partner personally and professionally commits to the findings and conclusions in any audit. The concurring opinion here refers to the external auditor's formal opinion, at the end of an audit, stating the client's financial reports are "fairly stated" in accordance with generally accepted accounting principles (GAAP).
- **Scope of internal control testing** . PCAOB rules require external auditors to describe the scope of testing processes and test findings. Prior to SOx, external auditors sometimes used internal firm policies to justify the most minimal of test sizes, and they often tested only a very small number of items despite being faced with very large test populations. If no problems were found, they expressed an opinion for the entire population based on the results of that limited sample. External auditors now must pay greater attention to the scope and reasonableness of their testing procedures, and the supporting documentation must clearly describe the scope and extent of testing activities.
- **Evaluation of internal control structure and procedures.** Although there were other standards during the first years of SOx, the PCAOB today requires use of AS 5 for the review and evaluation of internal controls. SOx rules further specify that an external auditor's evaluation must contain a description of material weaknesses as well as any material noncompliance matters found. External auditors are required to evaluate the effectiveness of an enterprise's internal controls. An absence of this documentation should be considered a weakness of internal controls.
- **Audit quality control standards.** While the PCAOB has not yet issued its own specific quality standards, SOx requires that every registered public accounting firm have quality standards related to:
  - Monitoring of professional ethics and independence
  - Procedures for resolving accounting and auditing issues within firm
  - Supervision of audit work
  - Hiring, professional development, and advancement of personnel
  - Acceptance and continuation of engagements
  - Internal quality inspections
  - Other quality standards to be proscribed by the PCAOB

These are very general quality standards, and over time the PCAOB will release a specific set of quality standards that apply to all registered public accounting firms. Likewise, we can also expect the IIA to establish quality standards applicable to all internal auditors. Quality standards based on the internationally recognized ISO 9000 are introduced in Chapter 31.

Some internal auditors might question the applicability of these PCAOB standards. Internal auditors have their IIA *International Professional Standards for the Practice of Internal Auditing* and may feel there is little need to become concerned here. However, PCAOB auditing standards impact business professionals and

internal as well as external auditors. With external auditors working under SOx rules, audit committees will expect both external and internal auditors to operate consistently. In the future, PCAOB rules may cause significant changes in the manner in which internal audits are planned, performed, and reported. Whether it is quality standards, effective internal controls testing, or concurrent approvals, an internal audit department should begin to modify its procedures to comply with the PCAOB standards.

(iii) INSPECTIONS, INVESTIGATIONS, AND DISCIPLINARY PROCEDURES The PCAOB conducts accounting firm inspections to assess compliance with SOx rules and professional standards; these occur annually at larger public accounting firms and once every three years if a registered firm conducts less than 100 financial statement audits yearly. The reviews evaluate the quality control system of the firm reviewed as well as their documentation and communication standards. The inspections are documented in formal reports to the SEC and state boards of accountancy. When appropriate, the PCAOB may initiate public accounting firm investigations and disciplinary procedures and can compel testimony, require the production of audit work, and conduct disciplinary proceedings. The latter may range from temporary suspension of an individual or firm, to substantial fines, or even to being barred from the profession.

The one brief paragraph on foreign public accounting firms in Title I's Section 106 has resulted in much controversy. It says that if any foreign public accounting firm prepares an audit report for an SEC-registered corporation, that foreign public accounting firm is subject to the SOx, the PCAOB, and related SEC rules, mandating those foreign firms must register under SOx rules. This has caused many problems. Our multinational world is filled with many non-U.S. public accounting firms, each governed by its own national public accounting standards. Most follow the international standards reporting standards (IFRS) that are similar but different from U.S. rules. We are now seeing some convergence in these standards, and as discussed in Chapter 30, the rules are changing.

(iv) ACCOUNTING STANDARDS Title I concludes by affirming that the SEC has authority over the PCAOB, including final approval of rules, the ability to modify PCAOB actions, and the removal of board members. While the PCAOB is an independent entity responsible for regulating the public accounting industry, the SEC is really the final authority. SOx recognizes the U.S. accounting standards-setting body, the Financial Accounting Standards Board (FASB), by saying that the SEC may recognize "generally accepted" accounting standards set by "a private entity" that meets certain criteria. The act then goes on to outline the general criteria that the FASB has used for setting accounting standards.

There is and always has been a major difference between accounting and auditing standards. The former define some very precise accounting rules, such as saying a certain type of asset can be written off or depreciated over no more than X years. These are the principles called generally accepted accounting principles. Auditing standards are much more conceptual, highlighting areas that an auditor *should consider* when evaluating controls in some area. During the 1990s, these auditing standards were loosely interpreted, as management was frequently under pressure to report short-term earnings growth and external auditors often refused to say no. The result was the financial scandals of Enron and others as well as Arthur

Andersen's destruction of audit documents when it received news that the SEC was coming. SOx and the PCAOB now oversee public accounting companies.

(b) Title II: Auditor Independence

Internal and external auditors are separate and independent resources, with external auditors responsible for assessing the fairness of an enterprise's published financial reports and internal auditors serving management in a wide variety of other areas. In the early 1990s, this separation began to change. External audit firms took responsibility for some internal audit functions as well. This process started when larger enterprises began to outsource some of their noncore functions, such as employee cafeterias or plant janitorial functions. The thinking was that employees working in these specialized areas were not really part of core enterprise operations, and all would benefit if people responsible for noncore functions were outsourced to another company that specialized in that particular area. The previous in-house janitors would be transferred to the janitorial services company and, in theory, everyone would benefit. The enterprise that initiated the outsourcing would experience lower costs by transferring a noncore function to a firm that better understood it. The outsourced janitor, in this example, also might have both better career possibilities and better supervision.

Internal auditor outsourcing started in the late 1980s following this same line of reasoning. External audit firms began offering to take over a client's existing internal audit functions. The idea made sense to senior management and their audit committees, which often did not really understand the distinctions between the two audit functions and were sometimes more comfortable with external auditors. Senior management and their audit committees also often were enticed by the promised of lower costs of internal audit outsourcing. Although the IIA initially fought against the concept, internal audit outsourcing continued to grow through the 1990s. A few independent firms adopted outsourcing, but internal auditor outsourcing occurred mainly in the major public accounting firms.

Internal audit outsourcing became an issue during investigations after the Enron failure. Enron's internal auditor function had been almost totally outsourced to its external audit firm, Arthur Andersen, and the two audit groups worked side by side in Enron's offices. After Enron's fall, after-the-fact questions were raised about how that outsourced internal audit department could have been independent of Andersen. Investigators felt it would have been very difficult in that environment for internal audit to raise any concerns to the audit committee about their external auditors. This potential conflict became a reform issue for SOx.

(i) LIMITATIONS ON EXTERNAL AUDITOR SERVICES SOx Section 201 forbids a registered public accounting firm from contemporaneously performing both audit and nonaudit services at a client. The prohibition includes internal auditing, many areas of consulting, and senior officer financial planning. It is now illegal for a registered public accounting firm to provide internal audit services if it is also doing a firm's audit work. Thus, the major public accounting firms are now out of the internal audit outsourcing business for their audit clients. Other firms, including independent spin-offs from public accounting firms, can still provide internal audit outsourcing, but the era of internal auditors becoming employees of their public accounting firm is over.

In addition to the ban on providing outsourced internal audit services, SOx prohibits public accounting firms from providing other services, including:

- **Financial information systems design and implementations.** Public accounting firms had been installing financial systems—often of their own design—at clients for many years. They then returned to review the internal controls of the systems they had just installed—a significant conflict of interest. This is no longer allowed.
- **Bookkeeping and financia statement services.** Public accounting firms previously offered accounting services to their clients in addition to doing the audits. Even for major corporations, it was not unusual for the team responsible for the overall financial statement audit also to do much of the work necessary to build those same consolidated financial statements. This potential conflict of interest also is no longer allowed.
- **Management and human resource functions.** Prior to SOx, external audit firms often helped their own professionals to move to client management positions. As a result, accounting managers in some enterprises often were alumni of their external auditors. This situation sometimes frustrated internal auditors or others who were not from that same public accounting firm, and avenues of promotion seemed limited because of old-boy network connections with the external audit firm.
- **Other prohibited services.** SOx also specifically prohibits external audit firms from offering actuarial, investment advisor, and audit-related legal services.

Under SOx, external auditors audit the financial statements of their client enterprises; that is about all. Beyond the prohibited activities, external auditors can engage in other nonaudit services only if those services are approved in advance by the audit committee. With the increased scrutiny of audit committees under SOx, many are wary of approving anything that appears to be at all out of the ordinary.

SOx external audit service prohibitions also have had a major impact on internal audit professionals. Because external audit firms can be *just the auditors,* internal audit professionals are finding increased levels of respect and responsibility for their role in assessing internal controls and promoting good corporate governance practices. Internal audit's relationship with audit committees also has been strengthened as the committees seek help for services that external audit firms sometimes assumed.

(ii) AUDIT COMMITTEE PREAPPROVAL OF SERVICES Section 202 of SOx's Title II specifies that the audit committee must approve all external audit and nonaudit services *in advance.* While most audit committees have been doing this all along, prior to SOx this approval was often little more than a formality. In the old days, audit committees often received little more than a brief report from their external auditors and then approved it in a perfunctory manner. SOx changed this. Audit committee members can expose themselves to criminal liabilities or stockholder litigation for allowing a prohibited action to take place. Of course, many minor external auditor activities do not have to go through formal audit committee approvals. Using legal terminology, SOx sets *de minimis*[2] exception rules for audit committee

permission requirements, stating that such permission is not required for nonauditing services if:

- The aggregate dollar value of the service does not exceed 5% of the total external audit fees paid by the enterprise during the fiscal year.
- The services were not recognized as nonaudit services by the enterprise at the time the overall audit engagement was initiated.
- These services are brought to the attention of the audit committee and approved by it prior to the completion of the audit.

These exceptions give an audit committee some flexibility, but the nature and accumulated dollar value of additional nonaudit services must be carefully monitored over the course of a fiscal year to maintain a level of compliance. Internal audit can help the audit committee to ascertain that all services continue in compliance with the SOx rules.

(iii) EXTERNAL AUDIT PARTNER ROTATION Title II makes it unlawful for a public accounting lead partner to head an engagement for more than five years. The major public accounting firms had corrected this well before SOx, and lead partner rotation had been common. SOx, however, makes the failure of a firm not to rotate a criminal act. Audit partner rotation sometimes challenges internal auditors who were working comfortably with a designated audit partner over extended periods.

(iv) EXTERNAL AUDITOR REPORTS TO AUDIT COMMITTEES While external auditors have always communicated with their audit committees in the course of the audit engagement, sometimes this communication was very limited. Management might negotiate a "pass" from their external auditors on some accounting change, but the matter would be reported to the audit committee only in the most general of terms if at all. External auditors are now required to report on a timely basis all accounting policies and practices used, alternative treatments of financial information discussed with management, the possible alternative treatments, and the approach preferred by the external auditor. If there are disputed accounting treatments, the audit committee should be made well aware of the actions taken.

(v) CONFLICTS OF INTEREST AND MANDATORY ROTATIONS OF EXTERNAL AUDIT FIRMS SOx Title II, Section 206, prohibits external auditors from providing any audit services to a firm where the chief executive officer (CEO), chief financial officer (CFO), or chief accounting officer participated as a member of that external audit firm on the same audit within the last year. In other words, an audit partner cannot leave an audit engagement to begin working as a senior executive of the firm that was just audited. There were some outrageous examples of this role-switching at Enron. The prohibition is now limited to public accounting partners; staff members and managers can still move to positions in the auditee enterprise. A common career path continues in which persons begin their careers in public accounting and then move to enterprise positions as members of internal audit.

(c) SOx Title III: Corporate Responsibility

While SOx Title II set up new rules for external auditor independence, Title III describes major new regulatory changes for audit committees. This is an area where

internal auditors should have a greater level of interest and role. Although audit committees were generally composed of independent directors, there were many exceptions. SOx introduced a wide range of governance rules covering corporate boards and their audit committees.

(i) **AUDIT COMMITTEE GOVERNANCE RULES** *All* registered enterprises must have an audit committee composed of only independent directors. The external audit firm reports directly to that audit committee, which is responsible for the firm's compensation, oversight of the audit work, and the resolution of any audit disagreements. While major corporations in the United States have had audit committees for some years, SOx has tightened and changed these rules a great deal. In addition, while internal audit sometimes had only a nominal reporting relationship to the audit committee, SOx now requires a strong, direct-line internal audit reporting relationship to the audit committee. Audit committee communications are discussed in Chapter 23.

SOx rules also call for audit committees to establish procedures to receive, retain, and treat complaints and to handle whistleblower information regarding questionable accounting and auditing matters. During the Enron debacle, an employee tried to get the attention of the external auditors or an Enron financial officer to disclose some improper accounting transactions, but the employee's concerns were rebuffed. An audit committee–led ethics whistleblower function could be a resource to respond to these types of issues. While not a normal audit committee responsibility, internal audit can potentially act as a conduit for SOx accounting and auditing whistleblower reports. Ethics and whistleblower programs, from an internal audit perspective, are discussed in Chapter 24.

(ii) **SECTION 302: CORPORATE RESPONSIBILITY FOR FINANCIAL REPORTS** Prior to SOx, enterprises filed their financial statements with the SEC and investors but, in the event of errors, the responsible corporate officers who signed those reports could argue they were not personally responsible for them. They could claim they did not understand the details and that any errors or problems were the responsibility of their subordinates. The bar has now been raised. The CEO, CFO, or other persons performing similar functions must personally certify each annual and quarterly report filed. The signing officer must certify that:

- The signing officer has reviewed the report.
- Based on that signing officer's knowledge, the financial statements do not contain any materially untrue or misleading information.
- Again based on the signing officer's knowledge, the financial statements fairly represent the financial conditions and results of operations of the enterprise.
- The signing officer is responsible for:
  - Establishing and maintaining internal controls.
  - Having designed these internal controls to ensure that material information about the enterprise and its subsidiaries was made known to the signing officer during the period when the reports are prepared.
  - Evaluating the enterprise's internal controls within 90 days prior to the release of the report.
  - Presenting in these financial reports the signing officer's evaluation of the effectiveness of these internal controls as of that report date.

- The signing officer has disclosed to the external auditors, audit committee, and other directors:
  - All significant deficiencies in the design and operation of internal controls that could affect the reliability of the reported financial data and, further, have disclosed these material control weaknesses to enterprise's auditors.
  - Any fraud, whether material or not, that involves management or other employees who have a significant role in the enterprise's internal controls.
- Have indicated in the report whether there were internal controls or other changes that could significantly impact those controls, including corrective actions, subsequent to the date of the internal controls evaluation.

Given that SOx imposes potential criminal penalties of fines or jail time on individual violators of the act, the signer requirement places a heavy burden on responsible corporate officers. Corporate officers must take all reasonable steps to make certain that they are in compliance.

This personal sign-off requirement has been a major concern for CEOs and CFOs. Enterprises need to establish detailed paper-trail procedures so that the signing officers are comfortable that effective processes have been used and the calculations to build the reports are all well documented. An enterprise may want to consider using an extended sign-off process where staff members submitting the financial reports sign off on what they are submitting. Internal audit should be able to act as an internal consultant and help senior officers establish effective processes here. The audit workpaper model, with extensive cross-references, might be a good approach. Exhibit 4.2 provides an example of an officer disclosure sign-off statement for senior officers. This exhibit is not an official PCAOB form but shows the type of letter an officer might be asked to certify and could be held criminally liable if incorrect. While the officer is at risk, the support staff—including internal audit—should take every step possible to make certain the package presented to the senior officer is correct.

Given SOx rules, internal auditors should take particular care regarding the nature and description of any findings encountered during the course of audits, on follow-up reporting regarding the status of corrective actions taken, and on the distributions of these audit reports. Many internal audits may identify significant weaknesses in areas of the enterprise that are not material to overall operations. A breakdown in the invoicing process at one regional sales office may be significant to the performance of that sales region for the corporation, for example, but it will not be a materially significant internal control weakness if the problem is local and does not reflect a wider, more pervasive problem, and if the problem was corrected after being discovered by internal audit. The chief audit executive (CAE) should establish good communications links with key financial officers in the enterprise such that they are aware of audits performed, key findings, and corrective actions taken. Internal audit should also provide some guidance as to whether reported audit findings are material to the enterprise's overall system of internal control. Similar communication links should be established with members of the audit committee.

(iii) IMPROPER INFLUENCE OVER THE CONDUCT OF AUDITS SOx makes it unlawful for any officer, director, or related subordinate person to take any action, in contravention of a SEC rule, to "fraudulently, influence, coerce, manipulate, or mislead" any external CPA auditor engaged in the audit for the purpose of rendering the financial

EXHIBIT 4.2 Sarbanes-Oxley Section 302 Officer Certification

Global Computer Products

Sarbanes-Oxley Section 302

Officer Certification

I, (*Name of Officer)*, certify that:

1. I have reviewed this quarterly report on Form 10-K of Global Computer Products;
2. Based on my knowledge, this quarterly report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this quarterly report;
3. Based on my knowledge, the financial statements, and other financial information included in this quarterly report, fairly present in all material respects the financial condition, results of operations, and the cash flows of, and for, the periods presented in this quarterly report;
4. The Global Computer Products' other certifying officers and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-14 and 15d-14) for the corporation and we have:
   a) designed such disclosure controls and procedures to ensure that material information relating to Global Computer Products, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this quarterly report is being prepared;
   b) evaluated the effectiveness of Global Computer Products disclosure controls and procedures as of a date within 90 days prior to the filing date of this quarterly report (the "Evaluation Date"); and
   c) presented in this quarterly report our conclusions about the effectiveness of the disclosure controls and procedures based on our evaluation as of the Evaluation Date;
5. The Global Computer Products' other certifying officers and I have disclosed, based on our most recent evaluation, to Global Computer Products and the audit committee of our board of directors (or persons performing the equivalent function):
   a) all significant deficiencies in the design or operation of internal controls that could adversely affect Global Computer Products ability to record, process, summarize and report financial data and have identified for Global Computer Products' auditors any material weaknesses in internal controls; and
   b) any fraud, whether or not material, that involves management or other employees who have a significant role in Global Computer Products' internal controls; and
6. Global Computer Products other certifying officers and I have indicated in this quarterly report whether or not there were significant changes in internal controls or in other factors that could significantly affect internal controls subsequent to the date of our most recent evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses.

statements materially misleading. These are strong words in an environment where earlier there was only a high level of discussion and compromise between auditors and senior management when a significant problem was found during an audit.

Prior to SOx, many "friendly" discussions between management and external auditors regarding a financial interpretation dispute or proposed adjustment resulted

in some level of compromise. This is not unlike an internal audit team in the field that circulates a draft audit report with local management before departing. After much discussion and sometimes other follow-up work, that draft internal audit report might be changed before its final issue. The same things often happened in external auditor draft reports covering quarterly or annual preliminary results. SOx rules now prohibit such practices. These rules evolved during the congressional hearings leading up to the passage of SOx, where testimony included tales of strong CEOs essentially demanding that external auditors accept certain questionable accounting entries or lose the audit business. Although there still can be friendly disputes and debates, if an SEC ruling is explicit and if the external auditors propose a financial statement adjustment because of that SEC rule, management *must* accept it without an additional fight.

There can be a fine line between management disagreeing with external auditors over some estimate or interpretation and management trying to improperly influence its auditors. External audit may have done some limited testing in some area and then proposed an adjustment based on the results of that test. This type of scenario could result in management disagreeing with that adjustment and claiming the results of the test were "not representative." While the external auditors under SOx have the last word in such a dispute, internal audit sometimes can play a facilitating role here as well. Internal audit resources, for example, can be used to expand the population of some audit sampling test, perform other extended observations, or perform other testing regarding the disputed area. Doing this, internal audit is not helping to improperly influence the conduct of an audit but helping to resolve the matter. AS 5 encourages these practices.

(iv) FORFEITURES, BARS, AND PENALTIES Title III concludes with a series of detailed rules and penalties covering corporate governance. Their purpose is to tighten existing rules that were in place before SOx or to add new rules for what often seemed to be outrageous or at least very improper business practices. These new rules, outlined next, do not impact the audit committee or internal or external auditors directly. They are directed at other areas of what was believed to be corporate governance excess.

- **Forfeiture of improper bonuses.** Section 304 requires that if an enterprise is required to restate its earnings due to some material violation of securities laws, the CEO and CFO *must reimburse* the company for any bonuses or incentives received on the basis of any original, incorrect statements issued during the past 12 months. The same applies for any profits received from the sale of enterprise securities during that same period. During the SOx hearings, multiple instances were cited where a company had issued an aggressive but unsupportable earnings statement, its key officers had benefited from bonuses or the exercise of stock options from that reported good news, and then the company soon had to restate its earnings due to some material noncompliance matter. Under the revised, correct interpretations, the CEOs and CFOs would not have received those bonuses. SOx places a personal penalty on senior corporate officers who benefit from materially noncompliant financial statements.
- **Bars to office or director service.** Section 305 is another example of how SOx has tightened up the rules. Prior to SOx, federal courts were empowered

to bar any person from serving as a corporate officer or director if that person's conduct demonstrates "substantial unfitness to serve as an officer or director." SOx changed the standard here by eliminating the word *substantial*. Now the courts can bar someone from serving as a director or officer for *any* conduct violation.

- **Pension fund blackout periods.** A standard rule for 401K and similar retirement plans has been that a fund administrator can establish a blackout period for fund administrative maintenance over a limited time period. While these blackouts are used to make changes to the overall fund, they prohibit plan participants from making investment adjustments to their plans during these restricted periods. A plan participant with a substantial amount of retirement funds in company stock could, because of bad company news, transfer funds from that company stock to a cash-based money market fund or some other investment option. These blackout periods are usually instituted for legitimate reasons, such as a change in plan administrators. An Enron-related complaint during the SOx hearings was that there was a blackout in place during the final weeks before Enron's bankruptcy, preventing employees from making changes to their plan. However, those same blackout rules did not apply to the corporate officers who had their own separate plan and who, in some cases, got out of the company plan before things totally collapsed. SOx rules now state that the same blackout periods must apply to everyone in the company, from staff to corporate officer.
- **Attorney professional responsibility.** Section 307 covers revised rules for attorney professional conduct and was initially very controversial. An attorney is required to report evidence of a material violation of securities law or a similar company violation to the chief legal counsel or the CEO. If those parties do not respond, the attorney is required to report the evidence up the ladder to the board audit committee. SOx's initial rules also allowed that if an attorney discovered such a securities law violation, the attorney should withdraw from the engagement and report the violation particulars to the audit committee or even the SEC, what is called a "noisy withdrawal" approach.

  The controversy here was that SOx effectively required an attorney to violate the rules of attorney-client privilege. Under traditional rules, if a subsidiary executive met with an attorney to discuss some matter that constituted a potential violation of SOx, the attorney and the subsidiary manager client would work out the issues. The initial concern was that an attorney was supposed to blow the whistle on such a discussion and bring the matter potentially all the way to the audit committee. The final rules, however, softened things to narrow the scope of the attorney's responsibility and otherwise limit the rules impact.
- **Fair funds for investors.** The final section of Title III states that if an individual or group is fined for a violation through administrative or legal action, the funds collected will go to a "disgorgement" fund for distribution to the investors who suffered because of the fraud or improper accounting actions. The same rule applies to funds collected through a settlement in advance of court proceedings. Properties and other assets seized will be sold and also go into that disgorgement fund. The whole idea here is that investors who lost because of individual corporate wrongdoing may be subject to some financial settlement from such a fund.

(d) Title IV: Enhanced Financial Disclosures

Title IV of SOx is designed to correct some financial reporting disclosure problems, to tighten up conflict-of-interest rules for corporate officers and directors, to mandate a management assessment of internal controls, to require senior officer codes of conduct, and other matters. There is a lot of material here. Many unexpected bankruptcies and sudden earnings failures around the time of the Enron failure were attributed to extremely aggressive, if not questionable, financial reporting. With the approval of their external auditors, many companies pushed to the limits and used such tactics as issuing questionable pro forma earnings reports or moving corporate headquarters offshore to minimize taxes. While these tactics were in accordance with GAAP and then existing laws, SOx tightened up many rules and made some improved financial disclosure tactics difficult or illegal.

Pro forma financial reports often were used to present an as-if picture of a firm's financial status by leaving out nonrecurring earnings expenses, such as restructuring charges or merger-related costs. However, because there is no standard definition and no consistent format for reporting pro forma earnings, depending on the assumptions used, it was possible for an operating loss to become a profit under pro forma earnings reporting. For example, in fiscal year 2001, Cisco Systems Inc., a San Jose, California–based maker of computer networking systems, reported net income of $3.09 billion on a pro forma basis but simultaneously reported a net loss of $1.01 billion on a GAAP basis. Cisco's pro forma profit specifically excluded acquisition charges, payroll tax on the exercise of stock options, restructuring costs and other special charges, an excess inventory charge, and net gains on minority investments. Cisco certainly was not alone here; many companies had reported pro forma earnings showing ever-increasing growth while their true GAAP results were not nearly as favorable. The problem with these two sets of numbers is that investors and the press frequently ignored the GAAP numbers, focusing on the more favorable pro forma results. SOx rules now require that pro forma published financial statements must not contain any materially untrue statements or omit any fact that makes the reports misleading. Further, the pro forma results also must reconcile to the financial conditions and results of operations under GAAP. A common reporting technique prior to SOx, pro forma results are not common today.

Perhaps the major issue that brought Enron down was a large number of off-balance-sheet transactions that, if consolidated with regular financial reports, would have shown major financial problems. Once they were identified and included with Enron's other financial results, the disclosure pushed Enron toward bankruptcy. SOx requires that quarterly and annual financial reports must disclose all such off-balance-sheet transactions that may have a material effect on current or future financial reports. These transactions may include contingent obligations, financial relationships with unconsolidated entities, or others. While many of the SOx financial disclosure rules are really the responsibility of external auditors, this is an area where internal auditors might be of help. Often the internal auditor, on a visit to a distant unit of the company, encounters these types of off-balance-sheet arrangements in discussions with field personnel. If the arrangements are significant, internal audit should communicate the appropriate details to the audit committee. SOx requires an enterprise to provide an explanation of its off-balance-sheet arrangements in a separately captioned subsection of the Management's Discussion and Analysis (MD&A) section of their annual Form 10K.

(i) EXPANDED CONFLICT OF INTEREST PROVISIONS AND DISCLOSURES The SOx legislative hearings often pictured corporate officers and directors as a greedy lot. In arrangements that often appeared to be conflicts of interest, large relocation allowances or corporate executive personal loans were granted and then subsequently forgiven by corporate boards. A CEO, for example, who requests the board to grant the CFO a large personal loan with vague repayment terms and the right to either demand payment or forgive certainly creates a conflict-of-interest situation. Although exceptions are allowed, SOx makes it generally unlawful for any corporation to directly or indirectly extend credit, in the form of a personal loan, to any officer or director.

Another section of Title IV requires that all disclosures under SOx must be filed electronically and posted "near real time" on the SEC's Internet site. This makes the filing of such information much more current. Internal audit should consider evaluating the control systems in place to handle such SEC online reporting. Reporting was often on hard copy in the past, and without proper internal control procedures, there could be a risk of improperly transmitted data or security leaks.

(ii) MANAGEMENT'S ASSESSMENT OF INTERNAL CONTROLS: SECTION 404 SOx requires that all annual 10K reports must contain an internal control report stating management's responsibility for establishing and maintaining an adequate system of internal controls as well as management's assessment, as of the fiscal year ending date, on the effectiveness of those installed internal control procedures. This requirement is known as the Section 404 rules. Internal audit, outside consultants, or even the management team—but not the external auditors—have the responsibility to review and assess the effectiveness of their internal controls. External auditors are then to attest to the sufficiency of these internal control reviews built and controlled by management.

Section 404 reviews are supported by the newly released AS 5 standards discussed in Section 4.3. These AS 5 rules are particularly important to internal auditors because the standards now specify that external auditors may elect to use the work of internal auditors in their internal controls reviews. An understanding of SOx Section 404 is an important element in every internal auditor's CBOK. As discussed in Chapter 28, internal auditors may act as consultants to their enterprises in helping to build these internal accounting controls or they can support external auditors by auditing those internal accounting controls.

(iii) FINANCIAL OFFICER CODES OF ETHICS SOx requires that enterprises adopt a code of ethics for their CEO, CFO, and other senior officers that discloses their compliance with this code as part of their annual financial reporting. While SOx has made this a requirement for senior officers, employee codes of ethics or conduct have been in place in some enterprises for many years. They evolved to more formal ethics functions in larger corporations in the early 1990s, but were often established only for employees and supervisors rather than for corporate officers. These codes defined a set of policies that were designed to apply for all employees, and they covered such matters as policies on the protection of company records or on gifts and other benefit issues. Exhibit 4.3 shows the table of contents of a sample enterprise code of conduct. Such a code of conduct should be designed for all enterprise stakeholders rather than just for the SOx-highlighted senior corporate officers.

With a growing public concern about the need for strong ethical practices, many enterprises have appointed an ethics officer to launch such an initiative along with a code of conduct as a first step. SOx has brought enterprise codes of conduct to

EXHIBIT 4.3 Enterprise Code of Conduct Sample Table of Contents

Topics Found in a Typical Enterprise Code of Conduct

I. INTRODUCTION
   - **A.** Purpose of This Code of Conduct: A general statement about the background of this Code of Conduct.
   - **B.** Our Commitment to Strong Ethical Standards: A restatement of the Mission Statement and printed letter from the CEO.
   - **C.** Where to Seek Guidance: A description of the ethics hotline process.
   - **D.** Reporting Noncompliance: Guidance for Whistleblowers—How to report.
   - **E.** Your Responsibility to Acknowledge the Code: A description of the code acknowledgement process.

II. FAIR DEALING
   - **A.** Our Selling Practice: Guidance for dealing with customers.
   - **B.** Our Buying Practices: Guidance and policies for dealing with vendors.

III. CONDUCT IN THE WORKPLACE
   - **A.** Equal Employment Opportunity Standards: A strong commitment statement.
   - **B.** Workplace and Sexual Harassment: An equally strong commitment statement.
   - **C.** Alcohol and Substance Abuse: A policy statement in this area.

IV. CONFLICTS OF INTEREST
   - **A.** Outside Employment: Limitations on accepting employment from competitors,
   - **B.** Personal Investments: Rules regarding using company data to make personal investment decisions.
   - **C.** Gifts and Other Benefits: Rules regarding receiving bribes and improper gifts.
   - **D.** Former Employees: Rules prohibiting giving favors to ex-employees in business.
   - **E.** Family Members: Rules about giving business to family members, creating potential conflicts of interest.

V. COMPANY PROPERTY AND RECORDS
   - **A.** Company Assets: A strong statement on the employees' responsibility to protect assets.
   - **B.** IT Systems Resources: An expansion of the company assets statement to reflect all aspects of computer systems resources.
   - **C.** Use of the Company's Name: A rule that the company name should be used only for normal business dealings.
   - **D.** Company Records: A rule regarding employee responsibility for records integrity.
   - **E.** Confidential Information: Rules on the importance of keeping all company information confidential and not disclosing it to outsiders.
   - **F.** Employee Privacy: A strong statement on the importance of keeping employee personal confidential to outsiders and even other employees.
   - **G.** Company Benefits: Employees must not take company benefits where they are not entitled.

VI. COMPLYING WITH THE LAW
   - **A.** Inside Information and Insider Trading: A strong rule prohibiting insider trading or otherwise benefiting from inside information.
   - **B.** Financial Reporting Disclosures: All accounting records as well as reports produced from those records will be produced in accordance with applicable laws as well as generally accepted accounting principles.
   - **C.** Political Contributions and Activities: A strong statement on political activity rules.
   - **D.** Bribery and Kickbacks: A firm rule of using bribes or accepting kickbacks.
   - **E.** Foreign Business Dealings: Rules regarding dealing with foreign agents in line with the Foreign Corrupt Practices Act.
   - **F.** Workplace Safety: A statement on the company policy to comply with OSHA rules.
   - **G.** Product Safety: A statement on the company commitment to product safety.
   - **H.** Environmental Protection: A rule regarding the company's commitment to comply with applicable environmental laws.

VII. COMPLIANCE WITH THIS CODE
   - **A.** All stakeholders are expected to comply with the letter and spirit of this code as well as applicable government rules and regulations.
   - **B.** Compliance with this code is a condition of employment.

new levels. It does not specify the content of enterprise-wide codes of ethics and focuses on the need for these standards to apply for senior officers. SOx specifically requires that an enterprise's senior officer code of ethics or conduct must reasonably promote:

- Honest and ethical conduct, including the handling of actual or apparent conflicts of interest between personal and professional relationships
- Full, fair, accurate, timely, and understandable disclosure in the enterprise financial reports
- Compliance with applicable governmental rules and regulations

If an enterprise has a code of conduct, management should ensure that it applies to all members of the enterprise, is consistent with SOx, and that these ethical rules are communicated to all members of the enterprise, including senior managers. An enterprise should make sure that its existing code of conduct covers the SOx rules, that it has been communicated to senior management, and that these officers have agreed to comply with it. While SOx compliance rules were established just for senior officers, this is the ideal time to launch an ethics function (discussed in Chapter 24) throughout the enterprise that applies to senior management and all employees. A strong ethics function should be promoted throughout the enterprise and not just as a SOx legal requirement.

(iv) OTHER TITLE IV REQUIRED DISCLOSURES All SEC-registered entities are required to file annual Form 10Ks as well as other SEC financial reports. The issuing enterprises filing those reports anticipate an SEC review in some detail; the hearings leading to SOx, however, revealed that these SEC reviews were not always timely or comprehensive. Section 408 mandates the SEC to perform "enhanced reviews" of the disclosures included in *all* company filings on a regular and systematic basis, and no less often than once every three years. The SEC can decide to perform an enhanced review of disclosures as soon as possible or to wait to schedule the review through the three-year window. This enhanced review could be triggered by *any one* of these situations:

- The corporation has issued a material restatement of its financial results.
- There has been a significant volatility in stock prices compared to others.
- The corporation has a large market capitalization.
- This is an emerging company with significant disparities in its stock price to earnings ratio.
- Corporation operations significantly affect material sectors of the national economy.
- Any other factors the SEC may consider relevant.

In essence, the SEC may schedule extended disclosure reviews for large Fortune 500 size companies, leaders in some sectors of the economy, or where stock prices are out of average ranges. Of course, with the "other factors" consideration, virtually any corporation could potentially move to the head of the list for such an extended review.

In general, these rules say that enterprises should be prepared for their public filings to be reviewed by the SEC more thoroughly and frequently than in the past. These financial statement disclosures are included in the MD&A section of

an enterprise's 10K report. This reporting covers a wide range of issues, including transactions with unaffiliated subsidiaries or derivative trading activities.

The last Title IV section, 409, mandates that enterprises must disclose "on a rapid and current basis" any additional information containing material financial statement issues. An enterprise can include trend and quantitative reporting approaches as well as graphics for those disclosures. This is a change from traditional SEC report formats, which allowed only text and corporate logos. The idea is to get key data to investors as soon as possible, not through slow paper-based reports. Section 409 points to the concept of a real-time financial close that soon may become a reality for many enterprises.

(e) Title V: Analyst Conflicts of Interest

This SOx title and other subsequent sections does not directly cover financial reporting, corporate governance, audit committees, or external or internal audit issues but was drafted to correct other perceived abuses encountered during the SOx congressional hearings. Title V is designed to rectify some securities analyst abuses. Investors have relied on the recommendations of securities analysts for years, but often these analysts were tied to large brokerage houses, and were analyzing and recommending securities to both investors and their financial institution employers. Regarding securities where their employer had an interest, there were supposed to be strong separations of responsibility between the people recommending a stock for investment and those selling it to investors. In the frenzy of the late 1990s investment dot-com bubble, these traditional analyst controls and ethical practices broke down. In the aftermath of the market downturns, analysts sometimes recommended stocks seemingly only because their investment bank employer was managing the initial public offering (IPO). Also, investigators found analysts publicly recommending a stock to investors as a "great growth opportunity" while simultaneously telling their investment banking peers that the stock was a very poor investment or worse.

Abuses of this manner existed in many circumstances. While investment analysts once relied on their own strong self-governing professional standards, the SOx hearings revealed that prominent securities analysts ignored many of these same standards. Title V attempts to correct these abuses. SOx has reformed and regulated the practices of securities analysts. Rules of conduct have been established with legal punishments for violations. The result should be better-informed investors.

(f) Titles VI through X: Fraud Accountability and White-Collar Crime

These SOx titles cover issues ranging from the funding of SEC appropriations to plans for future studies, and they include new rules to tighten up what had been viewed as past regulatory loopholes. Among these, the SEC can now ban persons from promoting or trading penny stocks because of past SEC misconduct or can bar someone from practicing before the SEC because of improper professional conduct. The latter rule gives the SEC the authority to effectively ban a public accounting firm from acting as an external auditor for corporations.

This SEC professional misconduct ban could be a major penalty to any public accounting firm or individual CPA that was found to have violated professional or ethical public accounting standards. Although SOx outlines a process of hearings before any action is taken, individual CPAs or entire firms can be banned temporarily

or permanently. The monitoring and policing processes have been taken away from the AICPA's peer review processes of the past and given to the SEC. While an individual negligent CPA can still work in non-SEC practice areas, such as small business accounting or internal audit, even a temporary ban can be a death knell for a practicing CPA or public accounting firm. All concerned must be aware of and follow SEC rules and procedures, particularly this new set authorized by SOx.

SOx Titles VIII and IX seem to be very much a reaction to the failure of Enron and the subsequent demise of Arthur Andersen. We have highlighted some of the events surrounding Enron's collapse, including the initial conviction of Arthur Andersen for its destruction of Enron's accounting records. At that time, even though Andersen seemed very culpable for its massive efforts to shred company accounting records, Andersen initially argued that it was just following its established procedures and had done no wrong. The courts eventually found Andersen innocent of criminal conspiracy, but the firm no longer exists. Title VIII of SOx has established specific rules and penalties for the destruction of corporate audit records.

The words in the statute apply to all auditors and accountants, including internal auditors. They are particularly strong regarding the destruction, alteration, or falsification of records involved in federal investigations or bankruptcies: "Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies or makes false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation ... shall be fined ... or imprisoned not more than 20 years, or both." Strong words taken directly from the statute! In other words, any enterprise should have a strong records retention policy. While records can be destroyed in the course of normal business cycles, any hint of a federal investigation or the filing of bankruptcy papers for some affiliated unit should trigger activation of that records retention policy.

A separate portion of this section establishes rules for corporate audit records. Workpapers and supporting review materials must be maintained for a period of five years from the end of the fiscal year of the audit. SOx clearly states that these rules apply to "any accountant who conducts an audit" of a SEC-registered corporation. In the past, internal auditors sometimes argued that they only do operational audits that do not apply to the formal financial audit process; nevertheless, the prudent internal audit group should closely align its workpaper record retention rules to comply with this SOx five-year mandate.

Several of the sections of the remaining SOx titles here were designed to tighten up some existing rules, sometimes viewed as excesses. One such excess was corporate officers getting large loans from their board of directors based on stock manipulation and performance that was later found to be improper. Boards of directors regularly forgave those loans after some period. Now SOx states that debts incurred in violation of securities fraud laws cannot be forgiven or discharged. The executive—now probably ex-executive—who received the forgiven loan is obligated to repay the corporation. Another section extends the statute of limitations for securities law violations. Now legal action may be brought no later than two years after discovery or five years after the actual violation. Since securities fraud can take some time to discover, this change gives prosecutors a bit more time.

The Organizational Sentencing Guidelines is a published list of corporate penalties for violations of certain federal laws. If an enterprise is found to be guilty, the punishment or sentencing could be reduced if an ethics program had been in place that should normally reduce the possibility of such a violation. While the basic

concepts of the sentencing guidelines are still in place, SOx modifies them to include the destruction or alteration of documents as offenses.

Section 806 adds whistleblower protection for employees of publicly traded enterprises who observe and detect some fraudulent action and then independently report it to the SEC or some other outside parties. By employees, we mean officers, contractors, or agents. Any person who observes an illegal act can blow the whistle and report the action with legal protection from retaliation. The SOx whistleblower rules cover securities law violations and do not include provisions in other federal contract whistleblower rules, where the person reporting a violation may receive some percentage of the reported recovery.

Title VIII's Section 807 defines criminal penalties for shareholders of publicly traded companies, stating that whoever executes or attempts to execute a scheme to defraud any persons in connection with a corporation's securities or fraudulently receives money or property from that sale "shall be fined or imprisoned not more than 25 years or both." This is a strong potential penalty for securities fraud. Title IX then goes through existing white-collar criminal law penalties and raises maximum punishments. For example, the maximum imprisonment for mail fraud has grown from 5 years to 20; maximum fines for violations have increased as well. These increased penalties coupled with the provisions of the Organizational Sentencing Guidelines create an environment where an increasing number of persons found guilty of white-collar crimes may have to spend time in prison.

Finally, Section 906 of SOx Title IX contains a requirement that CEOs and CFOs must sign a supplemental statement with their annual financial report that certifies that the information contained in the report "fairly represents, in all material respects, the financial condition and results of operations." These personal certifications have penalties of fines up to $5 million and 10 years imprisonment for anyone who certifies such statement while knowing it is false. Since these are personal penalties, the prudent CEO and CFO must take *extreme care* to make certain that all issues are resolved and that the annual financial statements are correct and fully representative of operations. Title X then is a "sense of the Senate" comment that corporate income tax returns must be signed by the CEO. Again, responsibility is placed on the individual officer, not the anonymous corporate entity.

(g) Title XI: Corporate Fraud Accountability

While prior sections of SOx focused on the individual responsibilities of the CEO, CFO, and others, this last SOx title covers corporate responsibilities for fraudulent financial reporting. Here the SEC is given authority to impose a temporary freeze on the transfer of corporate funds to officers and others in a corporation who are subject to an SEC investigation. This title was enacted to correct reported abuses where some corporations being investigated for financial fraud were simultaneously dispensing huge cash payments to individuals. A corporation in trouble should retain some funds until the matter is resolved.

Section 1105 also gives the SEC the authority to prohibit persons who have violated certain SOx rules from serving as corporate officers and directors. While the ban is not automatic, the SEC has the authority to impose it when appropriate. The idea is to punish the corporate wrongdoer who has been found culpable of securities law violations at one corporation and leaves that troubled corporation to serve at another.

4.2 Performing Section 404 Reviews under AS 5

Section 4.1 summarized the contents and requirements of the SOx legislation. It is an important law, and every internal auditor should have a general understanding of its content, a CBOK requirement. Going beyond just this general understanding, SOx's Section 404 on reviews of internal accounting controls should receive the most internal audit attention and understanding. In Section 404, an enterprise is made responsible for reviewing, documenting, and testing its own internal accounting controls, with those review results passed on to the enterprise's external auditors who are charged with then reviewing and attesting to that work as part of their audit of the reported financial statements. When SOx first became the law, Section 404 reviews were a major pain point for many enterprises because external auditors were following the financial accounting audit procedures defined in the PCAOB's Auditing Standard No. 2 (AS 2). These auditing standards required very detailed reviews that did not allow for small errors or omissions. The philosophy in the guidance was that an error is an error, no matter how large or small.

Starting in mid-2007, these Section 404 auditing rules were changed with the release of AS 5, a more risk-based audit approach that also allows external auditors to better use the work of internal auditors in their assessments. This section provides a summary of Section 404 rules and discusses approaches for performing reviews using AS 5's more risk-based approach. In addition, we look at approaches to keep supporting SOx Section 404 documentation up to date. SOx rules require that internal controls documentation should be updated on an ongoing basis, but this important requirement too often slips between the cracks. Business processionals and internal auditors need to understand the Section 404 rules and take steps to keep their enterprises in compliance. These rules impact both enterprises that have achieved SOx compliance in a previous period and those that are now just coming under registration requirements.

(a) Section 404 Internal Controls Assessments Today

Management has had an ongoing responsibility for designing and implementing internal controls over their enterprise's operations. Although the standards for what constituted good internal controls were not always that well defined in the past, they have remained a fundamental management concept. SOx Section 404 requires the preparation of an annual internal control report as part of an enterprise's SEC-mandated 10K annual report. In addition to the financial statements and other 10K disclosures, Section 404 requirements call for two information elements in each of these 10Ks:

1. A formal management statement acknowledging the enterprise's responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting
2. An assessment, as of the end of the most recent fiscal year, of the effectiveness of the enterprise's internal control structure and procedures for financial reporting

In addition, the external audit firm that issued the supporting audit report is required to review and report on management's assessment of its internal financial controls. Simply put, management is required to report on the quality of its internal

controls, and its public accounting firm must audit or attest to that management developed internal controls reports in addition to the normal financial statement audit. Management has always been responsible for preparing periodic financial reports; external auditors audited those financial numbers and certified that they were fairly stated. With SOx Section 404, management is now responsible for documenting and testing internal financial controls as well as reporting on their effectiveness. External auditors then review the supporting materials leading up to that internal financial controls report to assert that the report is an accurate description of the internal control environment.

To the nonauditor, this might appear to be an obscure or almost trivial requirement. Even some internal auditors who primarily perform operational audits may wonder about the nuances in this process. However, audit reports on the status of internal controls have been an ongoing and simmering issue among the public accounting community, the SEC, and other interested parties going back to at least 1974. Much of the problem then was that there was no recognized definition for the term *internal controls.* The release of the Committee of Sponsoring Organizations (COSO) internal controls framework in 1992 established an accepted standard for understanding internal controls. Under SOx Section 404, management is required to report on the adequacy of its internal controls; external auditors attest to the management-developed internal controls reports.

This process follows a basic internal control on the importance of maintaining a separation of duties where the person who develops transactions should not be the person who approves them. Under Section 404 procedures, the enterprise builds and documents its own internal control processes; then an independent party, such as internal audit, reviews and tests those same internal controls; and finally the external auditors review and attest to the adequacy of this overall process. The external audit procedures will be based on these internal controls. The Section 404 process improves things from pre-SOx days when external auditors frequently built, documented, and then audited their own internal controls—a separation of duties failing.

(b) Launching the Section 404 Compliance Review

(i) IDENTIFYING KEY PROCESSES Every enterprise uses a series of processes to conduct its normal business activities. Some may be represented by automated or information technology (IT) systems, others are primarily manual procedures performed on a regular basis, while still others are a combination of automated and manual. These processes generally are considered in terms of basic accounting cycles and include the:

- **Revenue cycle.** Processes dealing with sales or other revenue to the enterprise.
- **Direct expenditures cycle.** Covers expenditures of material or direct production costs.
- **Indirect expenditures cycle.** Covers operating costs that cannot be directly tied to production activities but are necessary for overall business operations.
- **Payroll cycle.** Covers all personnel compensation.
- **Inventory cycle.** Although inventory will eventually be applied to production as direct expenditures, special processes are needed due to the time-based holding nature of inventory until it is applied to production.

- **Fixed assets cycle.** Property and equipment require separate accounting processes, such as periodic depreciation accounting over time.
- **General IT cycle.** Covers IT controls that are general or applicable to all IT operations.

We discuss these same processes in Chapter 7 in the context of planning and performing effective internal audits. The identification of key processes is an initial Section 404 compliance step. Exhibit 4.4 describes a set of key processes for an example distribution company. *Process* is a term that often is used without too much thought to its meaning. A process is a particular course of action intended to achieve a result, such as an individual's process of obtaining a driver's license. It is a series of actions that have clearly defined starting points, consistent operational steps, and defined output points. We call this series of actions a process because they are a set of defined steps that can be repeated and followed consistently. A first compliance step here is to document, understand, and test key processes. During SOx's first years, many enterprises—often with the encouragement of their external auditors—attempted to define *every* process. There were no guidelines for eliminating the less risky ones. AS 5 has established a level of reasonableness here.

EXHIBIT 4.4 Key Processes for a Distribution Company Sample

1. **Purchase order management.** Processes must be in place to purchase or acquire the goods to be distributed.
2. **Inventory management.** Once goods have been purchased, processes are needed to manage them in inventory before distribution to customers.
3. **Warehouse management.** Processes must be in place to store product inventory in secure and well organized facilities, with subprocesses for the inspection and placement of goods.
4. **Demand planning.** An enterprise needs processes to know how customers will demand existing and new products. This may include marketing-based processes including customer surveys.
5. **Order processing.** Whether computer-based or paper-based, processes should be in place to receive new orders, approve customer credit histories, and pick and pack the received orders.
6. **Shipping and receiving.** Processes should be in place to ship to customers as well as to inspect and receive incoming ordered goods.
7. **Logistics management.** Processes are needed for special shipping arrangements, movement of goods between warehouse facilities, and other arrangements.
8. **Billing and invoicing.** After orders are received and shipped, processes are needed to bill customers for payment and then to manage those accounts.
9. **Accounting systems.** Beyond accounts receivable, an enterprise needs accounting and financial processes for all of its accounting functions.
10. **Information systems.** Processes are needed for all aspects of IT operations, including IT service design, service operations, delivery of all aspects of IT services, and processes for continual IT improvements.
11. **Human resources.** Processes are needed to manage all people associated with the distribution enterprise, including compensation, benefits, related taxes, and all human resource–based legislative legal requirements.
12. **Internal audit.** An effective internal audit function is needed.

Internal audit often can be a major help here. For many enterprises, internal audit may already have defined key processes through its annual audit planning and documentation. Such a process list should be developed to serve as a basis for launching a stream of internal controls reviews for the enterprise.

(ii) INTERNAL AUDIT'S ROLE Except for SOx's prohibition of external audit firms from performing internal audit services for audit clients, the original SOx legislation contains few specific references to internal audit. Nevertheless, internal audit has become an important resource in many enterprises today for the completion of Section 404 internal controls assessments. Under SOx, a separate and independent function within the enterprise—often internal audit—reviews and documents the internal controls covering key processes, identifies key control points, and then tests those identified controls. External audit then reviews that work and attest to its adequacy. For many enterprises, internal audit has been a key resource for performing these internal controls reviews. When SOx first became the law, internal audit functions often distanced themselves from Section 404 reviews because of internal auditor independence conflicts but to the then IIA professional standards. Changes in the IIA standards (discussed in Chapter 8) now allow internal auditors to act as consultants to help document and establish effective internal control processes. Internal audit's role in Section 404 reviews can take three forms:

1. Internal auditors can act as internal consultants for the enterprise by identifying key processes, documenting their internal controls, and performing appropriate tests of those controls. This review work would be subject to management approval for subsequent attestation by external audit.
2. Internal auditors can review and test internal control processes similar to their normal internal audit reviews but acting as assistants or contractors for external auditors. The enterprise could designate another in-house or outside consulting resource to perform the Section 404 reviews, and internal audit would act as a resource to support external auditors in reviewing the Section 404 work results. This approach is allowed under the AS 5 rules that allow external auditors to rely on internal audit materials.
3. Internal audit can work with and help other corporate resources, either internal or external, that are performing the Section 404 reviews but not get directly involved with those reviews, either as independent internal auditors or as agents for the external audit firm. This approach allows internal audit to devote more time and resources to other internal audit projects. This may also be the only alternative for a very small internal audit function.

The CAE, financial management, and the audit committee should work with the enterprise's external auditors to define responsibilities for these Section 404 internal control reviews. In some cases, it may be decided that it is most efficient for resources other than internal audit to act as assistants to the external auditors to perform these Section 404 reviews. External audit might make arrangements with internal audit to review and assess the adequacy of internal controls. In this situation, internal audit would be working for external audit in reviewing and attesting to the results of internal controls reviews but would not be performing the actual reviews. As mentioned, this type of arrangement will give internal audit an important role in helping external audit in achieving Section 404 review objectives. The negative

side of this arrangement is that the consultants assigned may not have the time, resources, or process knowledge to perform these assessments. This process often works best when an enterprise has another internal audit–like function, such as a strong quality assurance or risk assessment function, that can review, document, and test internal control processes.

Sometimes our first approach is best. Internal audit performs the review work for enterprise financial management for a subsequent but separate and independent assessment by the external auditors. The positive side of this arrangement is that internal audit is often the best and most qualified enterprise resource to perform these reviews. It understands internal controls and good documentation techniques. Although this arrangement involves more external audit resources, it may be an effective way to complete this Section 404 review requirement, but all parties must recognize their roles and responsibilities.

Whether for the first time or for ongoing updates, Section 404 reviews are an annual process, and internal audit can change its review strategy over the years. Documentation prepared and tested in the first year need only to be updated and retested in future periods. A company does not have to use the same strategy every year; however, changes always result in increased costs and added time spent re-learning approaches. All parties should develop a cost-effective approach to achieve these SOx requirements. While we are now taking a more risk-based approach under AS 5, the basic SOx Section 404 requirements have not changed.

(iii) ORGANIZING THE PROJECT Section 404 compliance places a major challenge on SOx-registered enterprises. Even though an enterprise has evaluated its internal controls using the COSO internal control framework, it will have some work ahead in documenting its internal controls environment. The more risk-based AS 5 approach to SOx today often makes the project somewhat easier. Whether in the first year or on an ongoing basis, internal audit can play a major role in helping senior management to get ready for Section 404 compliance. Based on the internal audit standards discussed in Chapter 8, internal audit should recommend internal control improvements as the new processes are being developed or can separately act as consultants for installing those new internal control processes.

Whether performed by internal audit or independent parties, Section 404 compliance reviews require a formal project based on the project management approaches discussed in Chapter 14. Larger SOx-registered public enterprises today have already gone through multiple rounds of SOx compliance work. Many smaller or foreign entities have not. The amount of effort required for new registrants is based on the strength and sophistication of an enterprise's internal control processes but should follow these eight steps:

Step 1: Organize the Section 404 compliance project approach. Assign a project team to lead the effort. A senior executive, such as the CFO, should act as the project sponsor with a team of both internal and external resources to participate in the effort. Roles, responsibilities, and resource requirements should be estimated as well. Internal audit can often assume major responsibilities here.

Step 2: Develop a project plan. The internal controls compliance project should be well in process prior to the financial year-end. While the existing plan can be updated in subsequent years, there will be a major challenge

EXHIBIT 4.5 Planning Considerations for a Section 404 Internal Controls Review

1. Determine status of review. Is this the first round of Section 404 reviews for the entity and a subsequent-year follow-up?
2. If a new review, follow the work steps to understand, document, and test key processes. Otherwise, plan for a subsequent-period review.
3. Review the detailed documentation covering prior Section 404 reviews, including process flowcharts, internal control gaps identified and remediated, and overall project planning documentation for prior review.
4. Review any recently published PCAOB rules covering Section 404 reviews and related auditing changes, and adjust review procedures to reflect those changes.
5. Meet with the external audit firm responsible for the current Section 404 attestations and determine is there are any changes in documentation and testing philosophy, with an emphasis on AS 5 rules, from that prior review.
6. Consider any organization changes since the past review, including acquisitions or major reorganizations, and modify review coverage, if necessary.
7. Through meetings with senior and IT management, determine whether new systems or processes have been installed over the past period and if those new changes have been reflected in updated documentation.
8. Review any internal control weaknesses identified in the past review and assess whether internal control corrections reported as installed appear to be working.
9. Assess the status of existing Section 404 documentation and determine the extent of new documentation preparation necessary.
10. Assuming the prior Section 404 review was done by internal audit, determine that appropriate knowledgeable trained resources are available to perform the upcoming review.
11. Interview all parties involved in the prior Section 404 review exercise to assess any lessons learned and develop plans for corrective actions in the upcoming review.
12. Based on discussions with external auditors and senior management, determine scope and materiality parameters for the upcoming review.
13. Determine that the software, if any, used to document prior review is still current, and make any changes necessary to have adequate tools in place to perform the upcoming review.
14. Prepare a detailed project plan for the upcoming Section 404 review, with considerations given to coordination of review activities at business entity units and external auditors.
15. Submit plan for approval by senior management.

and time crunch for earlier years. The plan should focus on significant areas of enterprise operations and cover all significant business units. Although there can be many plan variations here, Exhibit 4.5 outlines planning considerations for a Section 404 compliance review. Work steps described here are at a high level. The team should develop a detailed plan document to begin the SOx Section 404 internal financial controls review.

Step 3: Select key processes for review. Every enterprise depends on a wide range of financial and operational processes, but some processes possess greater risks than others. The payroll system, for example, is almost always a set of automated and manual routines that take time and attendance data and produce payroll checks or cash transfers to employee checking accounts. The total payroll process is much larger and includes steps necessary to add employees, process pay increases, and communicate with accounting and benefit systems. There can be numerous transaction flows in this overall

process. However, with every employee regularly checking his or her own compensation, most payrolls are highly controlled.

Internal audit and/or the Section 404 compliance team needs to review all enterprise processes and select the ones that are higher risk or financially significant. The selection should focus on processes where there is a risk that a failure could cause a major financial or operational risk to the enterprise. These processes should then be ranked by the size of assets controlled and other measures, with an overall consideration given to their risk of failure. Exhibit 4.6 contains some alternative factors to consider for this key process selection. For example, in raising the question of whether the application software was purchased or built in-house, the enterprise might—and probably should—decide that purchased software often has a lower risk. Internal audit can assist in developing documented procedures to justify why one process was more worthy or significant for detailed review than another. However, the enterprise should develop some risk-based criteria for why some process has or has not been selected for review. The approach should then be applied consistently.

Step 4: Document selected process transaction flows A next and important step is to prepare transaction flow documentation for the key processes selected. If documentation had been a previously prepared as part of a COSO internal controls review, it should be reviewed to determine if it is still accurate. Documentation can be much more of a challenge if this is a first-time SOx 404 review and if the enterprise has never documented its processes. There are a variety of accepted documentation protocols, and a goal should be to select some notation that is easy to prepare and update as well as easily understood by all interested parties. The documentation should show key transaction flows and control points in a manner that can support them on an ongoing basis. Three-ring notebooks full of process documentation are of little value if they are never updated. Enterprises should establish procedures to ensure that all changes to previously documented systems are updated when required. The groups or functions that initially documented these SOx processes should be given the responsibility to maintain them.

Documentation can be done as verbal descriptions, but it is usually best to use some type of flowcharting technique. The idea is to show the inputs, outputs, process steps, and key decision points for any process. Many different approaches can be used, and Chapter 16 contains some examples.

Step 5: Assess selected process risks. Once key processes have been defined and documented, the next step is to assess risks through a detailed "what could go wrong?" type of analysis. The idea is to ask questions about the potential risks surrounding each reviewed process. For example, in an accounts payable process, could someone gain access to the system and then arrange to cut himself an unauthorized check? Could system controls be sufficiently weak that multiple payments might be generated to the same authorized vendor? There could be numerous risks of this sort. The SOx review team should go through each of the selected processes and highlight potential risks using an open-ended set of questions and then focus on the expected supporting controls. Internal audit can play a very valuable role in this type of analysis.

EXHIBIT 4.6 Section 404 Process Review Selection Guidelines

The following questions can serve as a guide for selecting key processes to review as part of a Sarbanes-Oxley Section 404 review exercise. While there is no right or wrong answer to any of these, these should help the team selecting key processes to consider key factors.

I. **Process or System Status**
   A. Nature of the process or system to be reviewed:
      - Is this a new system or process developed in-house?
      - Is it a newly purchased application package?
      - Have there been major changes over past period affecting functionality?
      - Have past changes been described as only minor changes?
      - Is there adequate current documentation supporting the process?
   B. Past history of process or system changes:
      - Have there been significant changes over past two years?
      - Have changes been minor in the past two years?
      - Have there been two years or more since the last change?
      - Is this a new process or with no recent changes?
      - Is there an adequate document change control process in place?
   C. Process or system development team:
      - Is the development or management of the process handled by an outside contractor?
      - Is an in-house group responsible for process development and management?
      - Is the process a purchased packaged solution with only minor local changes?
   D. Top management interest in process of project:
      - Is this an enterprise-level process mandated by senior management?
      - Does the system or process responsibility reside at an operating-unit level?
      - Is this a process initiated by middle management?
      - Is this an individual user or departmental responsibility?

II. **Audit and Control Significanc**
   A. Type of system or process:
      - Does the process support financial statement balances?
      - Does it support major organizational operations?
      - Is it primarily for logistical or administrative support?
      - Is this a less critical statistical or research application?
   B. Past internal audit or SOx review involvement:
      - Has there been a prior SOx review, including control improvement recommendations?
      - Have prior reviews concluded with only limited recommendations?
      - Have prior Section 404 test results found no significant internal control problems?
      - If controls improvement recommendations have been made in prior reviews, do matters appear to have been corrected?
      - Is this a process that was never formally reviewed?
   C. System or process control procedures:
      - Are there process-generated internal controls?
      - Are there run-to-run controls with other systems or processes?
      - Is the process operating primarily in a batch mode or with manual controls?

III. **Impact of Process Failure**
   A. Impact of incorrect reported results. Would a process failure result in:
      - Potential legal liability?
      - Financial statement impact?
      - Potential for incorrect management decisions?
      - Limited decision support risks?
   B. Impact of application failure on personnel. Would a process failure result in a:
      - Need for extra management analysis time?
      - Need for extra user clerical time?
      - Need for a wide range of specialized resources?

Step 6: Assess control effectiveness through appropriate test procedures. System controls are of little value if they are not working effectively. Interviews and the preparation of process documentation sometimes can determine if appropriate controls are not in place or are ineffective. If so, the conclusions from the assessment should be documented and discussed with the process owners, and an action plan should be developed to take corrective actions to improve the controls.

In most instances, the documented controls should be tested to determine whether they are operating effectively. This audit testing has been a common process over the years for both internal and external auditor internal control reviews. At one time these audit tests were extremely extensive and expensive with large sample transactions sizes. Evaluation of the results of these samples allowed internal or external auditors to determine if financial results were fairly stated or internal controls appeared to be working. Statistically based audit sampling is less common today due to audit efficiency pressures as well as the lack of auditors with these skills. Chapter 9 provides an overview of statistical sampling for internal auditors.

Whether a statistically based sample is used or not, the SOx process reviewer should use one or more sample transactions to test whether controls are in place and working consistently. Exhibit 4.7 contains suggested sample sizes, based on the frequency of the control performance. If a control covers many repetitive items, the sample size to determine that it is operating effectively should be larger. The size of the sample can present a challenge for some processes, but in largely paper-based system, with many people-based approval steps, the SOx reviewer might borrow from other classic internal audit techniques and try a walk-through type of test. The idea here is to take a single transaction—such as a vendor invoice requiring approval—and individually walk that transaction through each of the of the processing steps prior to cutting the accounts payable check. Again, this is a test to assess internal controls over a process. If the results of the test are positive, the process reviewer could determine that the process appears to be working with adequate internal controls. This exercise is discussed in greater detail in Chapter 9 and should be part of an internal auditor's CBOK.

Step 7: Review compliance results with key stakeholders. Senior management is ultimately responsible for an enterprise's final Section 404 report. The project team should review its progress with senior management, highlighting review approaches and short-term corrective actions initiated. Similarly, since external auditors must formally attest to the results of this internal controls review, they should be kept informed of progress and any outstanding issues.

EXHIBIT 4.7 Recommended Sample Size by Control Frequency

Frequency the Control Operates	Recommended Minimum Sample Size
Multiple times per day	At least 30 items
Daily	At least 25 items
Weekly	At least 10 items
Monthly	At least 5 items
Quarterly	At least 2 items

Coordination with key stakeholders is important here. All too often, internal control assessments identify some potential weakness at a local facility, document it locally with little follow-up, and then raise it as a potentially significant weakness back at headquarters. In many cases, the potential weakness has minimal impact to the overall enterprise and could have been resolved and corrected at a local level. Stakeholder communication at all levels is important here.

Step 8: Complete the report on the effectiveness of the internal control structure. This is the final step in Section 404 compliance reviews, and this report, along with the external auditor's attest work, will be filed with the SEC as part of the enterprise's 10K annual report. All work should be documented similar to internal audit workpapers discussed in Chapter 16.

A first-time SOx Section 404 compliance project can be a major undertaking and certainly requires more time and effort than this list of work steps indicates. However, AS 5 rules have made this review process a bit easier. It is not necessary to go back to almost ground zero in each review cycle year; work from prior periods can be relied on. The old-timer, now experienced with multiple years of these reviews, might look at AS 5 and say something along the lines of "You should see how bad it was in the old days!" AS 5 has simplified and rationalized SOx internal control reviews, but these basic entity-level internal control review processes must remain in place.

As has been discussed, SOx Section 404 reviews are a key area where internal audit can play a very significant but often just an advisory role. The effort required will depend on the level of internal control work that has been performed earlier in the enterprise. Most larger major corporations have already gone through one or more cycles of these Section 404 reviews and are now in a maintenance mode. Often through the leadership of internal audit, these enterprises have reviewed, tested, and documented their internal controls following the COSO framework standard and now face the task of achieving Section 404 compliance on a continuing basis.

Also, if an automated system control was found to be effective in the first year and if there were no known changes to this process, it is no longer necessary to go back and redocument and retest in subsequent review periods. This is an example of exercising more of a risk-based approach. As another major change, management now has the flexibility to exercise judgment to tailor review approaches to enterprise facts and circumstances. Section 404 reviews continue to be important, but AS 5 rules offer more flexibility. We were often too detail oriented during SOx's first years; the objective under AS 5 should be to establish a more risk-based, reasoned approach to these assessments going forward.

4.3 AS 5 Rules and Internal Audit

Shortly after SOx became the law in the United States, the PCAOB released Auditing Standard No. 2 (AS 2), new guidance that called for external auditors to take very conservative and detailed approaches on their audits of financial statements. AS 2–mandated a look-at-everything detailed audit approach, and in those first years enterprise external audit bills were much more expensive. While many larger enterprises gritted their teeth and lived with the new rules, industry leaders, academics,

and others loudly proclaimed that AS 2 needed some revisions. The SEC and the PCAOB agreed to revise AS 2, with an objective of making the auditing standard more scalable for the 6,000 or more so-called nonaccelerated filers that had yet to comply with SOx as of 2007. Those publicly traded enterprises with a public float of $75 million or less were required to have their Section 404 auditor attestation reports completed in upcoming fiscal years, and many felt they needed some relief from AS 2 audit rules. As a result, Auditing Standard No. 5 (AS 5) was issued in late May 2007.

While AS 5 is really a set of standards for the external auditors who review and certify published financial statements, these new rules also are important for both internal auditors and financial managers. AS 5 introduces risk-based rules with an emphasis on the effectiveness of enterprise-level controls that are more oriented to enterprise facts and circumstances. In addition, this auditing standard calls for external auditors to consider including reviews of appropriate internal audit reports in their financial statement audit reviews. AS 5 allows external auditors to place more emphasis on management's ability to establish and document key internal controls. Both financial management and internal auditors need to understand these new risk-based and more scalable rules for the financial audits of their enterprises.

Although this book does not provide a total overview of AS 5 rules, a rule particularly important for internal auditors is that external auditors can now rely on the work of internal auditors in their Section 404 assessments.[3] Published in mid-2007 and just taking effect as this book is being published, AS 5 has four broad objectives:

1. **Focus internal control audits on the most important matters.** AS 5 calls on external auditors to focus their reviews on areas that present the greatest risk that an internal control will fail to prevent or detect a material misstatement in the financial statements. This approach calls for external auditors to focus on identifying material weaknesses in internal control in their audits, before they result in material misstatements of financial statements. AS 5 also emphasizes the importance of auditing higher-risk areas, such as the financial statement period-end accounting close process and controls designed to prevent fraud by management. At the same time, the new standard provides external auditors a range of alternatives for addressing lower-risk areas, such as by more clearly demonstrating how to calibrate the nature, timing, and extent of testing based on risk, as well as how to incorporate knowledge accumulated in previous years' audits into the auditors' assessment of risk. Also and very important to an internal auditor's CBOK, AS 5 also allows external auditors to use the work performed by an enterprise's internal auditors or financial staff, when appropriate.
2. **Eliminate audit procedures that are unnecessary to achieve their intended benefits** AS 5 does not include the previous AS 2 standard's detailed requirements to evaluate management's own evaluation process and clarifies that an internal control audit does not require an opinion on the adequacy of management's process. For example, AS 5 focuses on the multilocation dimensions of risk in an enterprise and reduces requirements that external auditors should test a "large portion" of an enterprise's operations or financial positions. This should reduce financial audit work.
3. **Make the audit clearly scalable to fi the size and the complexity of any enterprise.** In order to provide guidance for audits of smaller, less complex

companies, AS 5 calls for tailoring internal control audits to fit the size and complexity of the enterprise being audited. The standard has guidance on how to apply AS 5's principles to smaller, less complex enterprises as well as for the less complex units of larger enterprises.

4. **Simplify the text of the standard.** The new AS 5 is shorter and easier to read than its AS 2 predecessor, in part because the standard has been streamlined. It also has been reorganized to begin with the audit itself, with definitions and other background information presented only as appendices. For example, AS 5 eliminates the previous AS 2 standard's discussion of materiality, emphasizing that the auditor's evaluation of materiality is based on the same long-standing principles applicable to financial statement audits.

With AS 5, external auditors may consider using the work of others to help perform their SOx financial statement internal control assessments. This practice was not as well defined under previous SOx rules, but AS 5 states that an external auditor may use the work performed by, or receive direct assistance from, internal auditors, other company personnel, or third parties working under the direction of management or the audit committee to provide evidence about the effectiveness of financial reporting internal controls. This is a major change for internal auditors.

Of course, the external auditors are signing off on or attesting to the audit results, and they must assess the competence and objectivity of the persons who are performing work for them. The higher the degree of competence and objectivity of others helping with this external audit work, the greater the chance that an external auditor may use and rely on their work. In particular, AS 5 calls for an assessment of the competence and objectivity of internal auditors. *Competence* means the attainment and maintenance of a level of understanding and knowledge that enables persons to perform the tasks assigned to them, and *objectivity* means the ability to perform those tasks impartially and with intellectual honesty. To assess competence, an external auditor should evaluate the qualifications and ability of the internal auditors or others to perform the work the external auditor plans to use. To assess objectivity, AS 5 calls for an external auditor evaluation of whether factors are present that either inhibit or promote a person's ability to perform with the necessary degree of objectivity the work the auditor plans to use.

AS 5 goes on to state that external auditors should not use the work of persons who have "a low degree of objectivity, regardless of their level of competence," and also should not use the work of persons who have a low level of competence regardless of their degree of objectivity. Personnel whose core function is to serve as a testing or compliance authority at an enterprise, such as internal auditors, normally are expected to have greater competence and objectivity in performing the type of work that will be useful to an external auditor. The CAE and the audit committee and senior management may want to challenge external auditors who they see no role for internal audit in this SOx-related financial statement audit planning process.

Although AS 5 talks about internal auditors in an almost generic fashion, the role of the professional IIA member internal auditor is important here. Based on the *International Professional Standards for the Practice of Internal Auditing* (summarized in Chapter 8), an IIA internal auditor can be expected to have the competence and objectivity necessary for help in supporting an external auditor's review of Section 404 internal controls. Although other persons, such as outside consultants, can be used to assist external auditors in their financial statement internal control reviews,

internal auditors should have a major role in assisting with an enterprise's Section 404 and AS 5 audit compliance.

Internal audit's ongoing role here should be viewed with a level of caution. We have discussed how internal auditors often are excellent resources to identify, document, and test key Section 404 processes. They could do this in a support role for the external auditor's attestation reviews. However, pure separation-of-duties independence rules say that internal auditors cannot perform these reviews within the enterprise and then act as third-party helpmates for external auditors to help attest to that same work. This conflict of duties should be clearly understood by all parties, and care should be exercised by internal auditors and management to prevent it.

4.4 Impact of the Sarbanes-Oxley Act

The previous sections have provided a general overview of SOx. While this discussion did not cover all parts or details of the legislation, our intent is to give internal auditors an overall understanding of key sections that will have an impact on the financial statement annual audit of an enterprise and its audit committee. Whether a large, Fortune 100 U.S.-based corporation, a smaller company not even traded on NASDAQ, or a private company with a bond issue registered through the SEC, all will now or soon come under SOx and its public accounting regulatory body, the PCAOB. Internal auditors will see these changes in their dealings with their external auditors.

SOx has caused multiple changes to enterprises, both in the United States and worldwide. The roles and responsibilities of both external and internal auditors have changed, and enterprises certainly look at the internal controls and business ethics from a much different perspective. A general knowledge of SOx and its procedures for performing Section 404 internal controls reviews are important elements that should be in every internal auditor's CBOK repository.

Notes

1. The text of the law can be found in many Web locations. One source is http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf.
2. A principle of law: Even if a technical violation of a law appears to exist according to the letter of the law, if the effect is too small to be of consequence, the violation of the law will not be considered as a sufficient cause of action, whether in civil or criminal proceedings.
3. For more information on AS 5, see Robert Moeller, *Sarbanes-Oxley Internal Controls: Effective Auditing with AS 5, CobiT and ITIL* (Hoboken, NJ: John Wiley & Sons, 2008).

CHAPTER 5

Another Internal Controls Framework: CobiT

The internal controls framework of the Committee of Sponsoring Organizations (COSO), as introduced and discussed in Chapter 3, has become the standard mechanism for measuring and evaluating internal accounting controls under the Sarbanes-Oxley Act (SOx). However, SOx does not *mandate* the strict use of the COSO framework but only calls for its utilization for understanding and evaluating internal controls. Some professionals have expressed concerns about the COSO internal controls framework and have criticized it in particular because it does not give enough emphasis to information technology (IT) tools and processes. For example, the published COSO internal controls guidance materials look at IT application internal controls at a very high level; some have sought more IT-specific internal control guidance.

A more IT-oriented internal controls framework, called *C*ontrol *ob*jectives for *i*nformation and related *T*echnology (CobiT), was in place before SOx, and many enterprises began to use it when SOx became the law to comply with its Section 404 internal controls procedures. The CobiT internal controls framework provides guidance on evaluating and understanding internal controls, with an emphasis on enterprise IT resources. CobiT is not a replacement for the COSO internal controls framework but is a different way to look at internal controls in today's IT-centric world.

Although originally launched as a tool to help what were once called "computer auditors"—specialist internal and external auditors who reviewed IT-related internal controls—CobiT is a helpful tool for evaluating all internal controls across an enterprise. It emphasizes and provides guidance on the linkage of IT with other business resources to deliver overall values to an enterprise today. This chapter is an overview of the CobiT framework and its key components. More important, it describes the relationship between CobiT objectives and the COSO internal control framework for use in internal audit reviews. Even if they do not use the CobiT framework in reviews of internal controls, all internal auditors should have a high-level common body of knowledge (CBOK) of the basic CobiT framework. In addition to the COSO internal controls framework, knowledge of CobiT will help an internal auditor to better understand the role of IT controls and risks in many enterprise environments.

5.1 Introduction to CobiT

CobiT is an acronym that is becoming increasingly recognized by auditors and many IT professionals. Although sometimes abbreviated as COBIT rather than the correct designation as CobiT, the acronym or word stands for *C*ontrol *ob*jectives for *i*nformation and related *T*echnology. Because of this framework's emphasis on controls and technology, the first and last letters are capitalized. CobiT is an important internal control framework that can stand by itself but is an important support tool for documenting and understanding COSO and SOx internal controls. Although CobiT's original emphasis was on IT, the framework has been broadened. Auditors in many enterprises should at least have an understanding of the CobiT framework and its use as a tool for documenting, reviewing, and understanding SOx internal controls.

The CobiT standards and framework are issued and regularly updated by the IT Governance Institute (ITGI; www.itgi.org) and the closely affiliated professional organization, the Information Systems Audit and Control Association (ISACA). ISACA is more focused on IT auditing while ITGI's emphasis is on research and governance processes. ISACA also directs the Certified Information Systems Auditor (CISA) examination and professional designation as well as its newer Certified Information Systems Manager (CISM) certification and examination. These audit-related professional certifications are discussed in Chapter 27. ISACA was originally known as the Electronic Data Processing Auditor's Association (EDPAA), a professional group that was started in 1967 by internal auditors who felt their professional organization, the Institute of Internal Auditors (IIA), was not giving sufficient attention to the importance of IT systems and technology controls as part of internal audit activities. EDP once stood for electronic data processing, today an almost archaic term for IT. Over time, this professional enterprise broadened its focus and became ISACA, while the IIA has also long since embraced strong technology issues.

The EDPAA began to develop IT audit professional guidance materials shortly after its formation. Just as the EDPAA evolved into ISACA and now the ITGI, its original IT audit standards became an excellent set of internal control objectives that evolved to CobiT, now in its 2007 version 4.1 edition.[1] With virtually all enterprise processes today tied to IT-related matters, an understanding of the overall area of IT governance is critical. The CobiT framework is often described as a pentagon covering five broad and interconnected areas of internal controls, as illustrated in Exhibit 5.1. CobiT's major areas of emphasis are arranged around the important core concept of IT governance:

- **Strategic alignment.** Efforts should be in place to align IT operations and activities with all other enterprise operations. These include establishing linkages between enterprise business operations and IT plans as well as processes for defining, maintaining, and validating quality and value relationships.
- **Value delivery.** Processes should be in place to ensure that IT and other operating units deliver promised benefits throughout a delivery cycle and with a strategy that optimizes costs while emphasizing the intrinsic values of IT and related activities.
- **Risk management.** Management, at all levels, should have a clear understanding of an enterprise's appetite for risk, compliance requirements, and the impact

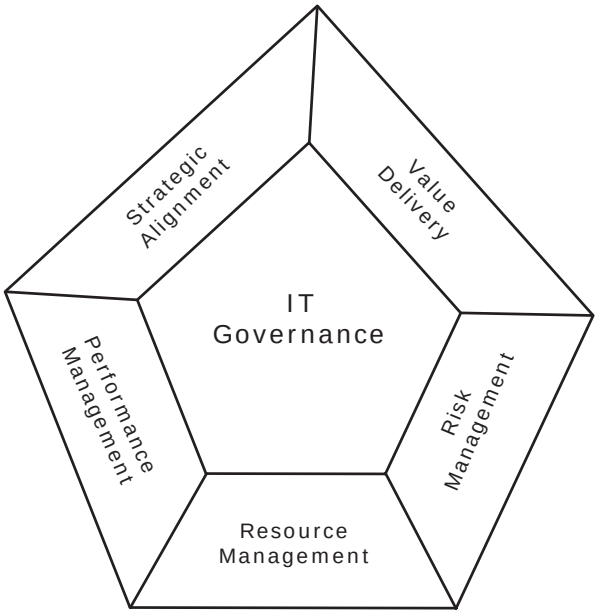


EXHIBIT 5.1 CobiT IT Governance Focus Areas

of significant risks. Both IT and other operations have their own and joint risk management responsibilities that may individually or jointly impact the entire enterprise.

- **Resource management.** With an emphasis on IT, there should be an optimal investment in, and the proper management of, critical IT resources, applications, information, infrastructure, and people. Effective IT governance depends on the optimization of knowledge and infrastructure.
- **Performance measurement.** Processes should be in place to track and monitor strategy implementation, project completions, resource usage, process performance, and service delivery. IT governance mechanisms should translate implementation strategies into actions and measurements to achieve these goals.

These five CobiT internal control concerns are the CobiT framework's elements and define IT governance. The CobiT framework is an effective tool for documenting IT and all other internal controls. This chapter looks at the framework in the broader perspective of using CobiT to assist in the IT governance processes of management, enterprise, and internal auditing.

The next sections provide an overall description of the CobiT framework and its key elements to link business with IT goals through key controls and effective measurement metrics. In addition, this chapter describes mapping CobiT standards with the COSO internal control framework, discussed in Chapter 3, the Information Technology Infrastructure Library (ITIL) Service Management best practices introduced in Chapter 18, and for overall IT and corporate governance. Elements and key components of IT governance are discussed as well. The CobiT framework is an effective mechanism for documenting and understanding internal controls at all

levels. Although CobiT first started primarily as a set of "IT audit" guidance materials, it is a much more powerful tool today.

5.2 CobiT Framework

IT processes and their supporting software applications and hardware devices are key components in any enterprise today. Whether a small retail business that needs to keep track of inventory and pay employees, or a Fortune 50 large corporation, all enterprises need a wide set of interconnected and often-complex IT processes that are closely tied to their business operations. That is, business processes and their supporting IT resources work in a close information-sharing relationship. IT cannot and certainly should not tell business operations what types of IT processes and systems they should consider implementing, but IT provides information to help influence business decisions. In the very early days of computer systems, IT managers sometimes felt they had lots of answers and promoted systems solutions to their businesses, sometimes with very counterproductive results. However, today this relationship has changed, and IT and business operations generally have a close mutual relationship of shared requirements and information. Internal auditors must understand the needs and information sharing requirements on both sides. IT has responsibilities over a series of other related process areas that are audited by or through established audit guidelines, are measured by a series of performance indicator measures and activities, and are made effective through a series of activity goals. All of these activities are part of CobiT, a control framework including both IT and business processes.

Chapter 3 described the COSO internal control framework and its importance in defining SOx internal controls. An internal auditor might say: "I understand and use COSO internals controls. Why use yet another framework?" The answer is that CobiT provides an alternative approach to define and describe internal controls that has more of an IT emphasis than the pure COSO internal controls framework. Information and supporting IT processes often are the most valuable assets for virtually all enterprises today, and management has a major responsibility to safeguard its supporting IT assets, including automated systems. Management, users of IT, and internal auditors all need to understand these information-related processes and the controls that support them. All of these users are concerned about the effectiveness and efficiency of their IT resources, the IT processes, and overall business requirements, as shown in Exhibit 5.2 describing these basic CobiT principles. In the exhibit, business requirements drive the demand for IT resources, and those resources initiate IT processes and enterprise information in a continuous circular manner. Management should be interested in the quality, cost, and appropriate delivery of its IT-related resources whose control components are the same as the COSO internal control elements. Internal controls over IT resources are very much based on the effectiveness and efficiency interdependencies of these IT components.

IT governance is a key CobiT concept that, prior to SOx, was not strongly emphasized as a CobiT element. It is an important internal control concept today with the ITGI playing a strong leadership role. As described in Exhibit 5.1, CobiT defines IT governance as a series of key areas ranging from keeping focus on strategic alignments to the importance of both risk and performance measurement

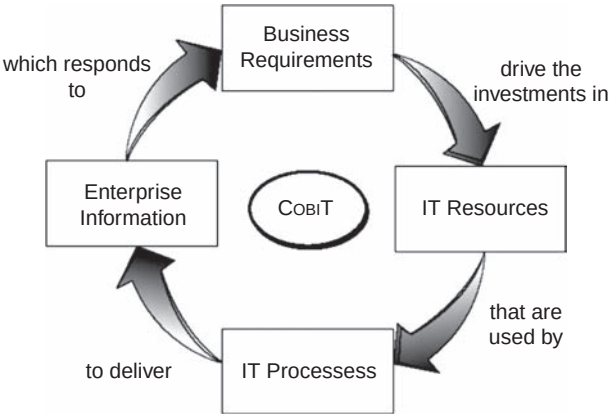


EXHIBIT 5.2 Basic CobiT Principles

Source: Control Objectives of Information Related Technology (CobiT®), Third Edition. Copyright © 1996, 1998, 2000, the IT Governance Institute®, http://isaca.org and http://itgi.org, Rolling Meadows, IL 60008, USA. Reprinted by permission.

when managing IT resources. We will see references to this IT governance pentagon as we navigate through the CobiT framework to better understand internal controls framework.

CobiT also looks at controls in three IT-related dimensions: resources, processes, and information criteria. These three are also described in what is called the CobiT cube, as illustrated in Exhibit 5.3. Similar to the COSO internal controls framework cube from Chapter 3 and the COSO ERM framework from Chapter 6, this CobiT model looks at IT controls from a three-dimensional perspective. That is, each

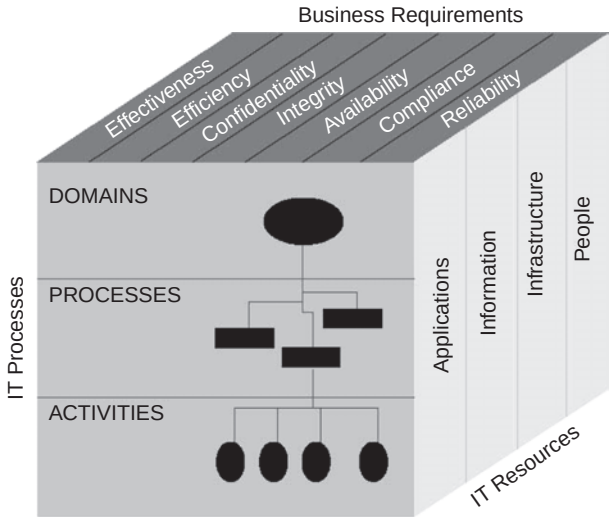


EXHIBIT 5.3 CobiT Cube

Source: CobiT 4.1 © 1996–2007. All rights reserved. Used by permission.

component on one plane relates to its two other connecting dimensions. However, CobiT's front-facing dimension with its pictorial descriptions of process flow diagrams has sometimes scared off non-IT people. The non-IT-savvy professional—and there are many—may look at the process diagrams and decide this approach must be "too technical." This is not at all correct. The next sections explain the CobiT framework and why it can be valuable for understanding SOx internal controls and improving IT governance.

(a) CobiT Cube Components: IT Resources

The IT Resources side of the three-dimensional CobiT cube represents all of an enterprise's IT assets, including its people, the application systems, installed technology, its facilities, and the value of data. Looking at Exhibit 5.3, this side of the cube represents the concerns for all of the resources necessary for the operation of enterprise IT resources. Either individually or as groups, these resources should be considered when evaluating controls in an IT environment, identified as:

- Applications consisting of both automated user systems and manual procedures to process information
- Information, including input, output, and processed data, for use by business processes
- Technology and facility infrastructure components including hardware, operating systems, databases, networks, and the environments that house and supports them
- Key and specialized personnel to plan, organize, acquire, implement, support, monitor, and evaluate IT services

We have started our CobiT description from the right-hand side of the cube, but control considerations must always be considered in terms of how they relate to components on the other sides of the cube. The point here is that IT resources should always be considered as a key component of IT governance and internal controls.

(b) CobiT Cube Components

(i) IT PROCESSES The second and front-facing dimension of the CobiT cube references IT Processes and consists of three segments: domains, processes, and activities. Domains are groupings of IT processes that match to organizational areas of responsibility; CobiT defines four specific domain areas:

1. **Planning and enterprise.** This domain area covers the strategy and tactics that allow IT to best contribute to and support enterprise business objectives. This type of IT strategic vision message should be communicated throughout the enterprise—the message of IT's mission and what it is trying to accomplish for the overall enterprise. These are IT-specific materials similar to the Chapter 24 discussion on ethics.
2. **Acquisition and implementation.** IT solutions need to be identified, developed or acquired, and both implemented and integrated with business processes. This domain area covers changes and maintenance of existing systems.

3. **Delivery and support.** This domain area covers the actual delivery of required services, both the application and infrastructure tools. The actual process of application data and controls is covered within this domain.
4. **Monitoring and evaluation.** This area includes control processes, including quality and compliance monitoring, as well as external and internal audit evaluation procedures.

Within an IT enterprise, the process to identify and build new applications—often called systems development life cycle (SDLC) procedures—could be viewed as part of the CobiT implementation domain with quality assurance a part of the monitoring domain. The CobiT descriptive materials describe each of these domain areas in greater detail:

- Define a strategic IT plan.
- Define the information architecture.
- Determine technological direction.
- Define the IT enterprise and relationships.
- Manage the IT investment.
- Communicate management aims and direction.
- Manage human resources.
- Ensure compliance with external requirements.
- Assess risks.
- Manage projects.
- Manage quality.

Individual processes are the next level down. They are joined activities with natural control breaks. Finally, activities are the actions needed to achieve measurable results. Activities have a life cycle whereas tasks are discrete. By *life cycle,* we can think of the systems development life cycle (SDLC) process where a new application is first designed, implemented, then operated over time, and finally replaced with an improved process.

(ii) **BUSINESS REQUIREMENTS** The third dimension of the CobiT cube is described as Business Requirements. Its seven components should be considered for all business requirements with consideration given to the necessary IT resources and processes:

1. Effectiveness
2. Efficiency
3. Confidentiality
4. Integrity
5. Availability
6. Compliance
7. Reliability

All IT overall systems should be evaluated based on these seven areas. Emphasis will vary depending on the type of process, but all IT processes should have these criteria in mind. Business functions typically establish such requirements for general

business needs and for IT. Each of these attributes is discussed in more detail in Section 5.3 and in Chapter 18 on auditing IT general controls using ITIL.

The CobiT cube presents an effective way to understand the relationships among business requirements, IT processes, and IT resources. The three-dimensional nature of the model emphasizes the cross-relationships and interdependencies between business and IT processes. In our IT-dependent world, this is a useful way for an internal auditor to look at and understand internal controls. CobiT is a rich—sometimes almost too rich—set of processes for focusing on business and IT goals and key controls and identifying key measurement metrics. The next sections discuss CobiT in some high level of detail, but the reader is encouraged to consult the IT Governance Institute's CobiT materials for more details and explanations.

5.3 Using CobiT to Assess Internal Controls

In addition to the CobiT cube, with its forward face showing process flow diagrams to emphasize relationships, the published CobiT guidance material[2] can look formidable to some internal auditors and many business and even IT professionals. The basic CobiT reference material is published in a nearly 200-page manual filled primarily with an array of charts and tables. It is a useful set of materials, but some study may be required to fully understand the concepts behind the CobiT framework. The sections here should help an internal auditor to navigate through the published CobiT framework and, more important, use it to develop and assess enterprise internal controls.

Although any dimension of the CobiT cube can be used to understand control environments, the four previously discussed domains, starting with planning and enterprise, serve as an effective first step. Based on these three CobiT control cube dimensions, each IT process should be evaluated through five navigation steps in this way:

I The control of (*process name*)
II Which satisfy (*list of business requirements*)
III By focusing on (*list of important IT goals*)
IV Is achieved by (*list of control statements*)
V And is measured by (*list of key metrics*)

This five-step process can go from number I down or can start at the base level and navigate up. In either case, the CobiT framework says that the control of any process should be satisfied by a list of supporting business requirements and that those business goals should focus on important IT goals. This makes sense. A designated process would just be a name unless specific business and IT requirements drive and govern that process. Each of those requirements should be defined by one or more control statements with specific control practices. Finally, we cannot assess whether matters are operating effectively and key measurement metrics are necessary.

This five-step process can be a script for understanding controls supporting any process in the enterprise. The important element here is defining the number IV control statements supporting each process and the number V identification of metrics to assess those identified controls. Although CobiT's emphasis has historically

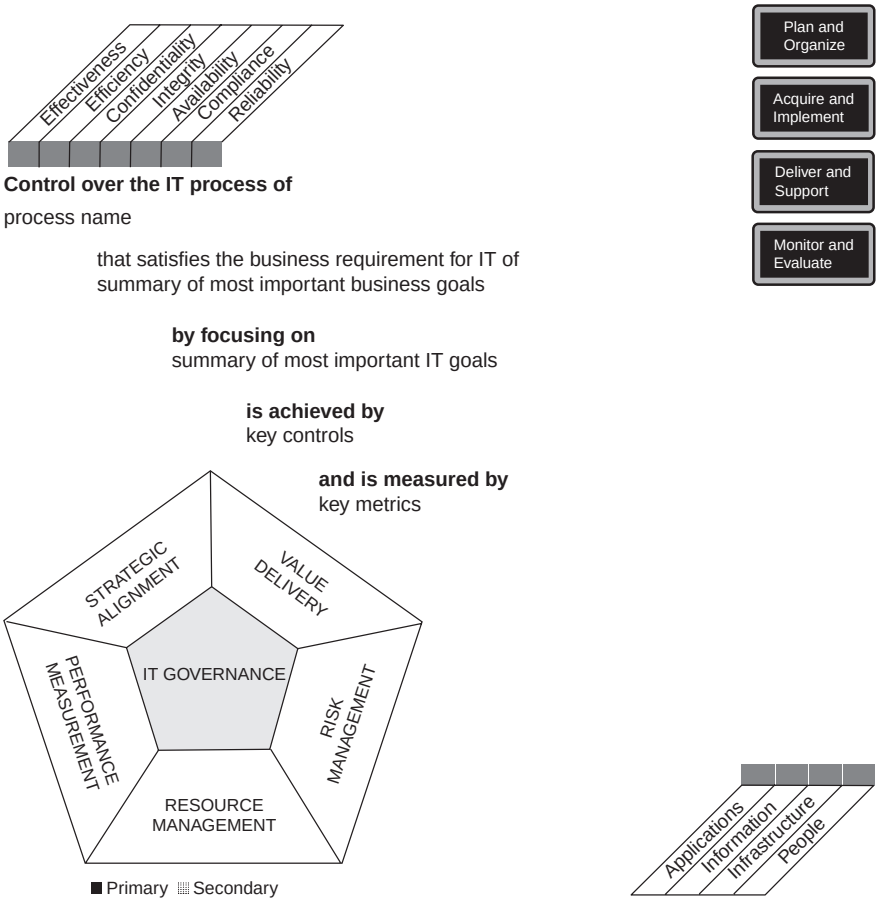


EXHIBIT 5.4 Steps for Navigating the CobiT Framework

Source: CobiT 4.1 © 1996–2007 ITGI. All rights reserved. Used by permission.

been on IT, this type of analysis should be used for a wide range of internal control–related audits, whether IT related or not.

Each major control objective in the published CobiT guidance material is based on the ITGI's navigation framework shown in Exhibit 5.4. The upper left corner of that exhibit shows business requirements. While this is a blank sample, in the published CobiT guidance, each is marked with a P (for a primary requirement), S (for secondary), or left blank for a not applicable control objective. The lower right-hand corner lists the IT resource areas. If any are applicable, they are noted with a check mark. The lower left corner shows the same pentagon diagram shown in Exhibit 5.1. Here sections are shaded or marked if they are of primary or secondary importance.

The center of each of the CobiT guidance pages has the "Control over the IT Process of" series of statements completed for each control objective. We show examples of completed statements as we review the CobiT domains later. Even though the CobiT navigation and supporting documentation is thorough and really quite elegant, it can also scare away the first-time internal auditor.

Next we look at CobiT navigation across various selected domains to give a feel for its organization. Internal auditors should at least experiment with using CobiT in selected internal audits. This chapter provides an introduction and overview to CobiT; its supporting ITGI professional organization has a wide variety of published and educational offerings on the use of CobiT that can be found on the Web site, www.isaca.org.

(a) Planning and Enterprise

CobiT calls for a high-level group of processes that set the direction for the enterprise and its IT resources. For this domain, CobiT calls for 10 high-level Planning and Organizing (PO) control objectives, defined and numbered in this way:

PO1 Define a strategic plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define IT process, enterprise, and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.

These are all very high-level concepts where many managers might argue, "Of course!" when an internal auditor uses this list to ask whether they have a strategic plan, have defined their information architecture, or are in compliance with any of these PO objectives. However, CobiT drills down its defined control objective areas in greater detail. While many of the issues are similar, this is in strong contrast to the Monitoring element of COSO internal controls as discussed in Chapter 3. There, the concepts are only at a fairly high level; CobiT is much more specific. For example, using this PO1 control objective on defining a strategic plan, CobiT then describes six more detailed objectives under PO1:

PO1.1 IT value management.
PO1.2 Business-IT alignment.
PO1.3 Assessment of current performance.
PO1.4 IT strategic plans.
PO1.5 IT tactical plans.
PO1.6 IT portfolio management.

The numbering here is important, as the published CobiT guidance materials references each of these and other objectives in terms of their inputs and outputs. CobiT's published materials provide a high-level description for each of these objectives. For example, the PO1.4 objective on strategic plans states:

> *Create a strategic plan that defines, in co-operation with the relevant stakeholders, how IT will contribute to the enterprise's strategic objectives (goals) and related costs and risks. It includes how IT will support IT-enabled investment*

programs and operational service delivery. It defines how the objectives will be met and measured and will receive formal sign-off from the stakeholders. The IT strategic plan should cover investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements. The strategic plan should be sufficiently detailed to allow the definition of tactical IT plans.

This paragraph is an example of one of the many control objectives in the CobiT guidance. They do not tell the professional *how* to write an IT strategic plan but provide excellent guidance on how to build such a plan, no matter the size or status of the enterprise. These general objectives are also good tools for internal auditors who need to build review criteria in any of these areas. Those audit objectives can be developed by taking each sentence of such a control objective and developing audit review areas.

For each of the CobiT objectives, the guidance material also contains what is called a RACI chart. A tool that evolved from quality initiatives in the 1960s, a RACI chart is good tool to identify process roles and responsibilities. Using a spreadsheet format, activities are identified in a side column with functions or position descriptions in cells across the top. Responsibilities for those activities are identified in intersecting cells through one or several of the RACI initials:

R = Responsible, or owns the problem or process.
A = Accountable, or who must sign off on the activity before it is effective.
C = Consulted, or who has the information and/or capability to complete the work.
I = Informed, or who must be informed of the results but need not be consulted.

This type of chart can be useful to help identify responsibilities over multiple areas. Exhibit 5.5 is a RACI chart, adapted from CobiT materials, on the PO1 objective to define a strategic IT plan. Going down the column of responsibilities, in this example, the Business Process Owner is *R*esponsible for analyzing program portfolios,

EXHIBIT 5.5 RACI Chart for Defining a Strategic IT Fit

CobiT P01 Activities	CEO	CFO	Business Executive	CIO	Process Owner	Head of Operations	Head IT Admin	Internal Audit
Link Business Goals to IT Goals	C	I	A/R	R	C			
Identify Critical Dependencies and Current Performance	C	C	R	A/R	C	C	C	C
Build an IT Strategic Plan	A	C	C	R	I	C	C	C
Build IT Tactical Plans	C	I		A	C	C	C	I
Analyze Program Portfolios and Manage Service Portfolios	C	I	I	A	R	C	C	I

is *I*nformed on processes for building the strategic plan, and acts as a *C*onsultant on other activities for this control objective. The chart outlines responsibilities for such people as the enterprise's head of IT or chief information officer (CIO), the process owner, and internal audit. This type of RACI chart appears in the published guidance for each of the CobiT control objectives.

The CobiT material concludes with a summary analysis of its control objective. For each, a metrics-based set of considerations outlines the control activity goals, measured by a set of key performance indicators (KPIs) that drive process goals. The latter drive IT goals that are measured by IT key goal indicators. This process and the set of CobiT documentation are explained as we review the other CobiT control objectives.

For the PO major control objective, the guidance material discusses each control objective in the same manner and following the same approach as for the high-level controls review approaches. Many of these CobiT items may be found only in larger IT functions, although the CobiT guidance material has a range of approaches for each objective. For example, the CobiT objective PO3.5 identifies the need for an IT architecture board or function. This is valuable guidance, but many smaller IT resources will not have the resources to establish such a formal IT architecture board function. Managers who use CobiT and auditors who evaluate compliance should always recall that CobiT is a set of best practices guidance materials but not mandatory requirements. Internal auditors should always use the CobiT guidance with some caution, recognizing that CobiT often specifies some very high-level ideals An internal auditor who follows CobiT to the letter and recommends the need for a formal "IT Architecture" board in a smaller enterprise could get laughed out of someone's office.

(b) Acquisition and Implementation

Each of the CobiT high-level control objectives discuss control procedures in the same general format. Whether it is in-house software development efforts or purchased IT components, the recommended high-level acquisition and implementation objectives here are:

AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.

Each of the detailed objectives in this domain covers control procedures over the implementation of new tools. While the emphasis is on IT software, the internal control concepts can be applied to the acquisition and implementation of many new enterprise tools.

Space does not allow complete discussion of each control objective, but we will examine AI6 on managing change as an example of how CobiT outlines this control area. For example, earlier we outlined CobiT's five-step process for evaluating

control objectives. The outline for these steps appears in the center of the Exhibit 5.4 navigation page. The AI6 objectives on managing change follow the same five-step process:

I. Control over the IT Process of managing change

II. That satisfies the business requirement for IT of responding to business requirements in alignment with business strategy, while reducing solution and delivery defects and rework

III. By focusing on controlling impact assessment, authorization, and implementation of all changes to the IT infrastructure, applications, and technical solutions, minimizing errors due to incomplete request specifications and halting implementation of unauthorized changes

IV. Is achieved by

- Defining and communicating change procedures, including emergency changes
- Assessing, prioritizing, and authorizing changes
- Tracking status and reporting on changes

V. And is measured by

- Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment
- Application or infrastructure rework caused by inadequate change specifications
- Percent of changes that follow internal change controls processes.

This series of statements, taken from the CobiT guidance materials, describes the control requirements and measures for this specific AI6 control objective. The CobiT guidance materials have a similar set of statements for each control objective, which is useful when attempting to better understand the characteristics of each control.

That same guidance material looks at how each control objective relates to the other two sides of the CobiT cube. For the AI6, Manage Changes, control objective, it indicates that on the IT Resources side, all are important. That is, the control object impacts Applications, Information, Infrastructure, and People. Turning to the upper left side of the navigation sheet Business Requirements dimension, the guidance material indicates whether they are Primary, Secondary, or of no significant importance. For this AI6 example control objective, the Business Requirements of Effectiveness, Efficiency, Integrity, and Availability are of primary importance while Reliability is of secondary importance. The remaining two requirements, Confidentiality and Compliance, are not considered significant to this control objective.

For each control objective, the CobiT guidance material shows an image of the Exhibit 5.1 focus areas pentagon. For this AI6 control objective, Value Delivery is of prime importance with Resource Management secondary. The CobiT guidance material does not provide any detailed discussion of the reasons for that designation. The professional working with any of the CobiT control objectives usually can deduce why a given IT governance area has been designated as of primary or secondary significance.

(c) Delivery and Support

Following the same general format, the third high-level CobiT control objective is called Delivery and Support (DS). This control objective largely covers service management issues related to the ITIL business process objectives discussed in Chapter 18. This really highlights some of the changes to our understandings of internal controls that have evolved since the enactment of SOx in 2002. Both CobiT and ITIL were with us at that time, but the SOx Section 404 emphasis on effective internal controls has brought things together. The CobiT DS control objectives are similar to the ITIL internal controls to enhance business processes. Both cover the important area of what is known as IT service management, processes required to ensure efficient IT operations and to deliver these services.

In earlier days, concerns about IT internal controls often focused on individual application-by-application controls. While much attention was given to the higher-level general controls such as perimeter security or disaster recovery planning, auditors and others often focused on the computational and balancing controls in specific applications. However, no matter how well designed, all such IT applications must operate in an efficient, automated factory–like atmosphere. There will always be such smaller problems, however, such as a legitimate systems user being locked out by entering incorrect passwords. There is a need for efficient service and problem management processes to report and resolve such matters. The CobiT DS control objectives cover many of these important areas:

DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.

These control objectives represent important areas of IT operations that historically often have not received sufficient attention. The CobiT material summarizes how each control objective is achieved and measured and considers the relationships and interdependencies across all three sides of the CobiT cube.

Many of these control objective areas did not received sufficient attention in internal controls reviews prior to SOx Section 404. COSO objectives address internal controls at a high level but sometimes do not focus on more detailed service management–related internal control issues. The CobiT DS10 control objective for problem management is an example:

> *Effective problem management requires the identification and classification of problems, root cause analysis and resolution of problems. The problem management process also includes identification of recommendations for improvement,*

maintenance of problem records and review of the status of corrective actions. An effective problem management process improves service levels, reduces costs, and improves customer convenience and satisfaction.

For years, IT users have had problems using various systems and applications, but insensitive IT operations frequently have not done an appropriate job in resolving reported problems. All too often, if a major application totally fails, there is a strong effort to get it back in operation. Smaller, less critical problems, however, are brushed off as something to be "considered in the next update."

The published CobiT guidance material links this control objective to others that provide its inputs as well as outputs. For example, the objectives of AI6 on change authorization, DS8 for incident reporting, DS9 for IT configuration management, and DS13 on error logs all provide inputs to the DS10 control objective. Here we do not reproduce the full contents of the published CobiT control objectives but give the reader a feel for its approach. CobiT provides a powerful way to look at the breadth and depth of IT-related internal controls and their relationships.

We have discussed how each CobiT control has a series of detailed objectives, has other control inputs and outputs, and has a RACI chart outlining functions and responsibilities for each control. In addition, the published CobiT guidance materials have a Goals and Metrics section for each control objective. Exhibit 5.6 shows this chart for the DS10 Manage Problems control objective. Each published CobiT control objective has a similar set of these very useful analyses. With problem management, for example, three suggested measurement metrics should be considered. One of these is performing a root cause analysis of reported problems, an important goal that is sometimes missed. The related RACI chart highlights that the problem manger is responsible for this activity while others have a consulting role.

Under each activity goal, a table of key performance indicators follows that drive a set of process goals. With different specific contents for each CobiT control, this type of analysis provides all parties with a good set of standards for measuring the performance of control areas and establishing metrics to assess achievement of these goals. This analysis for problem management is a good example of the power of the published CobiT materials. Many IT operations have some types of "help desk" function to report and resolve problems. Here CobiT provides good suggestions for the types of measures and metrics that can be used to evaluate the achievement of this control objective.

Similar tables of goals and objectives exist for each control objective. These are similar to the SOx auditing standards discussed in Chapter 4 or the internal audit professional practice standards referenced in Chapter 8. However, the CobiT materials provide excellent guidance materials for establishing and then measuring effective internal controls.

(d) Monitoring and Evaluation

The fourth CobiT domain is called Monitoring and Evaluation (ME), a set of control objectives that emphasize CobiT as a closed-loop process that effectively never ends. CobiT calls for establishing baseline measures to allow an enterprise to measure how they are performing and to provide them with opportunities in future periods. This domain area covers quality assurance areas that traditionally have been more common to manufacturing and other operations areas than to IT.

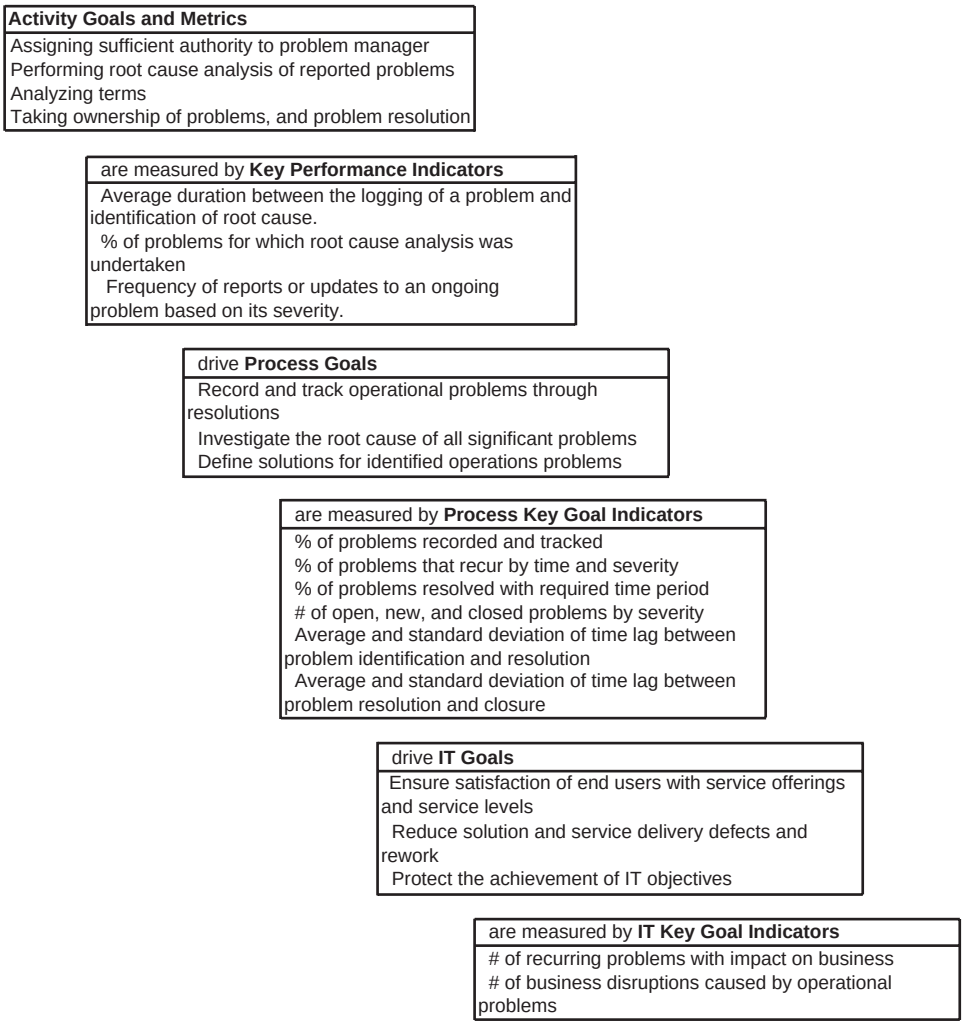


EXHIBIT 5.6 CobiT Example: DS10 Manage Problems Goals and Metrics

Although not discussed in the CobiT guidance materials, the pioneering quality assurance work of W. Edwards Deming provides a way of considering this CobiT domain area.

A consultant helping to rebuild Japan in the aftermath of World War II, Deming developed quality standards and approaches that helped Japan rebuild and establish the quality practices that are used worldwide today. Among other approaches, Deming developed a quality system approach that called for business processes to be analyzed and measured to identify the sources of variations that cause products to deviate from customer requirements. He proposed that business processes be placed in a continuous feedback loop so that managers could identify and change parts of the process that needed improvement. This should be a continuous, never-ending cycle where we should always monitor current process performance and take

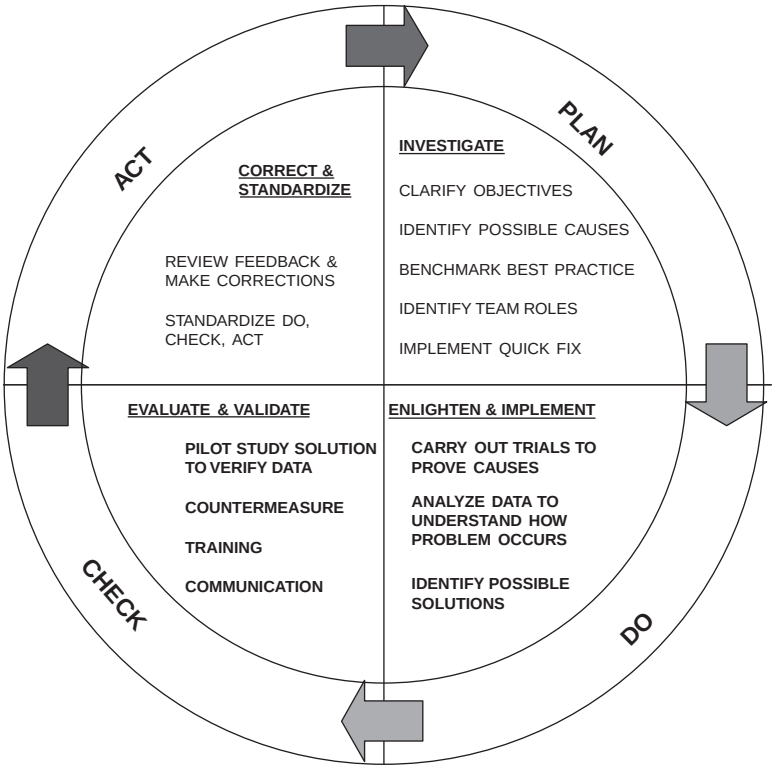


EXHIBIT 5.7 Deming's PDCA Cycle

Source: Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, COBIT, and ITIL. Copyright © 2008, John Wiley & Sons. Reprinted with permission of John Wiley & Sons, Inc.

actions to implement improvements to that process. Deming called this the Plan, Do, Check Act cycle (PDCA), as shown in Exhibit 5.7. The steps here are:

Step 1. Plan: Design or revise business processes to improve results.
Step 2. Do: Implement to plan and measure its performance.
Step 3. Check: Assess the measurements and report the results
Step 4. Act: Decide on needed changes to improve results.

Although Deming's focus was on postwar reconstruction and on industrial production, his concepts have been carried forward and are very appropriate for today's business environments, including IT operations and SOx internal control monitoring.

Following the same format as the other CobiT domains, the ME domain component has four principle control objectives:

ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal controls.
ME3 Ensure regulatory compliance.
ME4 Provide IT governance.

This area is of particular interest to internal auditors as well as members of the enterprise outside of IT operations. The control material for ME2 on monitoring and evaluating internal controls is a good example of CobiT's strength. It states that the process of monitoring and evaluating internal control is achieved by defining the system of IT controls embedded in the IT process framework, by monitoring and reporting on the effectiveness of these internal controls, and by reporting exceptions to management for corrective action. This is really the Deming PDCA process, and it should be measured by:

- Number of internal control breaches
- Number of control improvement initiatives
- Number and coverage of control self-assessments

As with most of the CobiT framework, the material here focuses on IT controls, but many of these concepts can be generalized to an overall internal controls review process. *Control self-assessments* refer to the process of ongoing internal reviews on the completeness and effectiveness of one's internal controls. They are an important internal audit process discussed and are outlined in Chapter 11.

This CobiT Monitor and Evaluate Internal Controls objective has seven detailed supporting objectives. Here we summarize them to describe their essence. While CobiT is oriented to internal reviews of these primarily IT resource areas, this guidance is important for internal auditors in the reviews of all other internal controls:

ME2.1 Monitoring of the Internal Control Framework. Internal auditors should continuously monitor the control environment and framework using industry best practices and benchmarking to improve the control environment and framework.

ME2.2 Supervisory Review. In addition to auditor reviews, CobiT calls for management to monitor and report on the effectiveness of IT internal controls through supervisory reviews, including compliance with policies and standards, information security, change controls, and controls established in service-level agreements.

ME2.3 Control Exceptions. Record information regarding all control exceptions and ensure that it leads to analysis of the underlying cause and to corrective action. Management should decide which exceptions should be communicated to the individual responsible for the function and which exceptions should be escalated.

ME2.4 Control Self-Assessments. IT management should evaluate the completeness and effectiveness of the internal controls over their IT processes through a continuing program of self-assessment.

ME2.5 Assurance of Internal Control. IT should obtain, as needed, further assurance of the completeness and effectiveness of internal controls through third-party reviews by the corporate compliance function, internal audit, outside consultants, or certification bodies.

ME2.6 Internal Control at Third Parties. Assess the status of each internal external provider's internal controls and confirm that they comply with legal and regulatory requirements and contractual obligations.

ME2.7 Remedial Actions. Identify and initiate remedial actions based on the controls assessments and reporting. This includes follow-up of all assessments including: (1) review, negotiation, and establishment of management responses; (2) assignment of responsibility for remediation or risk acceptance; and (3) tracking the results of the actions taken.

These CobiT control objectives are described as "detailed" but provide openings for a wide range of even more control procedures. For example, ME2.1 on monitoring the internal control framework calls for internal auditors to develop detailed control procedures that typically may result in a program of many more tests or steps.

This CobiT control objective, as well as all of the others in the supporting documentation, has a section on assessing the maturity of each internal control. *Maturity* here refers to the Capability Maturity Model (CMM; sometimes called CMMi, where the *i* stands for the integration of process areas and best practices). CMMi is a five-level assessment measure designed and developed by Carnegie Mellon University.[3] The model has defined levels for when controls can be assessed from a CMMi level 1 of nonexistent, level 2 as initial or ad hoc controls all the way to level 5, optimized controls. CobiT rates each of its controls against this CMMi measure. For example, CobiT defines that an enterprise will be at Level 3, defined process controls for ME2, Monitor and Evaluate Internal Controls, when management supports and has institutionalized internal control monitoring. The guidance goes on to say that policies and procedures should have been developed for processing and reporting internal control monitoring activities. To achieve this CMMi level, an educational and monitoring program for internal control monitoring should have been defined.

The published CobiT materials have a limited set of CMMi maturity-level guidance materials for each of their internal controls. Although summarized at a very high level, these maturity model guidelines allow an enterprise to assess how it is doing with regard to each of CobiT's internal controls.

5.4 Using CobiT in a SOx Environment

When SOx first became effective in the United States, there was little guidance on how to implement and manage its Section 404 internal controls reviews. The PCAOB initially indicated that it was going to establish some specific standards but left enterprises and their external auditors on their own. Many enterprises adopted CobiT, with its heavy emphasis on high-level IT-oriented internal controls, as the internal control framework of choice. This section reviews using the CobiT framework to help achieve SOx compliance.

Chapter 4 discussed SOx Section 404 internal controls assessment requirements and highlighted risk-based approaches for evaluating internal controls with an emphasis on the COSO internal controls framework. CobiT is a powerful alternative internal controls assessment framework, particularly in environments with a heavy concentration of IT processes and resources. As discussed, both COSO internal controls and CobiT use three-dimensional cubical frameworks to describe their internal control environments. They are similar but with slight differences in classifications and terminology, Exhibit 5.8 shows how the CobiT framework maps to the COSO internal controls model. CobiT's prime objectives, from Planning and Enterprise to

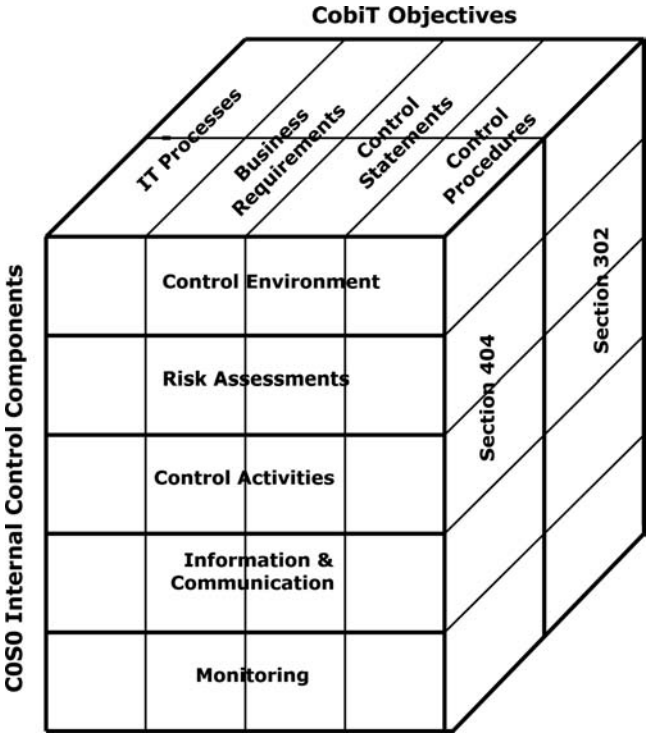


EXHIBIT 5.8 Relationship between COSO Components and CobiT Objectives

Monitoring and Evaluation, can be used to understand and evaluate internal controls through COSO's five internal control components. Whether considering COSO internal controls in general or using CobiT, an internal auditor should move through a series processes from planning to performing risk assessments and on to identifying, documenting, and evaluating key internal controls.

With SOx, the increased emphasis on IT governance, and the recognition of the criticality of IT in most internal control decision, CobiT has gone through multiple revisions until the current 4.1 edition. CobiT's sponsoring IT Governance Institute has been doing an excellent job releasing publications that map the CobiT framework to these other standards. For example, there is a very detailed study[4] that maps the CobiT framework to SOx audit requirements. Exhibit 5.9 is an extract of this published CobiT guidance showing how major CobiT control objective areas links with the major COSO components of internal control. This link-up ties together even better by going a level lower. For example, CobiT objective AI6 on Managing Changes under the Acquire and Implement control domain impacts the COSO components of Control Activities and Monitoring. The published CobiT detailed control objectives tie to each of these COSO components. There is a close relationship between these CobiT and COSO control objectives and components.

The full set of CobiT control objectives materials provides strong support for an internal auditor performing a SOx Section 404 internal controls assessment review. While the concepts can be used in any internal control area, the emphasis is on IT applications and processes. For many enterprises, an understanding and assessment of those IT-associated internal controls is key to achieving SOx compliance. CobiT

EXHIBIT 5.9 COSO and CobiT Relationships

	COSO Components				
	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
Plan and Organize COSO Control Objective					
Define a strategic IT plan		X		X	X
Define the information architecture			X	X	
Determine technological direction					
Define the IT organization and relationships	X			X	
Manage the IT investment					
Communicate management aims and directions	X			X	X
Manage human resources	X			X	
Ensure compliance with external relationships			X	X	X
Assess risks		X			
Manage projects					
Manage quality	X		X	X	X
Acquire and Implement COSO Control Objective					
Identify automated solutions					
Acquire and maintain application software			X		
Acquire and maintain technology infrastructure			X		
Develop and maintain procedures			X	X	
Install and accredit			X		
Manage changes			X		X
Deliver and Support COSO Control Objective					
Define and manage service levels	X		X		X
Manage third party services	X	X	X		X
Manage performance and capacity	X		X		
Ensure continuous service	X		X		X
Ensure systems security	X		X	X	X
Identify and allocate costs	X		X	X	X
Educate and train users	X		X		

(Continued)

EXHIBIT 5.9 COSO and CobiT Relationships *(Continued)*

	COSO Components				
	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
Assist and advise customers					
Manage the configuration	X		X	X	
Manage problems and incidents			X	X	X
Manage data			X	X	
Manage facilities			X		
Manage operations			X	X	
Monitor and Evaluate COSO Control Objective					
Monitor the processes				X	X
Assess internal control adequacy					X
Obtain independent assurance	X				X
Provide for independent audit					

has been around for some years now, but many had viewed it as just a specialized IT audit tool, not as more general help for other internal audit work. Although CobiT's emphasis continues to be on IT, all internal auditors should consider the CobiT framework as an excellent tool for helping with current and evolving SOx compliance requirements.

5.5 CobiT Assurance Framework Guidance

While the CobiT framework provides guidance for establishing effective internal controls with an emphasis on IT resources, the ITGI in 2008 released its Information Technology Assurance Framework (ITAF)[5] guidance, a good-practice-setting model to provide guidance on the design, conduct, and reporting of IT audit and assurance assignments. The objective of this CobiT-related guidance is to establish standards for IT audit and assurance professional roles and responsibilities, knowledge and skills, and diligence, conduct and reporting requirements. Our title and many references in this book use the word *auditing*; this new CobiT guidance focuses on another and less common audit-related word, *assurance*. This term is also found in IIA basic references that state:

> *Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.*[6]

As is discussed in Chapter 29, assurance covers all forms of internal auditing, risk management, and compliance services. This CobiT guidance covers a wide range of reviews performed by an internal auditor.

The overall objective of an ITAF is to define a set of standards to help ensure the quality, consistency, and reliability of IT assessments, based on a set of good practice-setting guidelines and procedures. While the ITAF document refers to its guidance as "standards," at this time CobiT's ISACA is not recognized as a standards-setting body. Chapter 8 outlines the IIA standards and summarizes CobiT-related ITAF standards. We mention these new ITAF standards here to highlight the fact that internal auditing standards are being developed to help with reviews in a CobiT environment. However, an internal auditor should understand that ITAF is new; it may achieve more recognition as it becomes better accepted and perhaps fine-tuned.

5.6 CobiT in Perspective

Whether operational, financial, or IT specialists, all internal auditors should have at least a high-level CBOK understanding of the CobiT framework. It is a particularly useful tool for assessing internal controls in a more IT-oriented environment—the type of environment that we almost always encounter today. The decision to use CobiT in internal audits should not be a one-time or individual audit level decision. Rather, internal audit should train key members of the audit team on the use of CobiT, then try using it to assess internal controls on some other audit being developed and documented using internal audit techniques discussed in Chapters 7 and 9.

For many enterprises, CobiT will offer some improvements to ongoing audit processes. Its application should first be discussed with the audit committee to explain the reasons for changing internal audit approaches. If the enterprise places a heavy reliance on IT systems and processes, the move to using CobiT seems good logistically. However, internal audit should not have IT internal audit specialists using CobiT assessment processes while the rest of internal audit uses established operational/financial internal audit standards.

CobiT is an elegant—sometimes too elegant—internal control framework and evaluation tool for assessing internal controls. Perhaps the largest internal audit impediment to its overall use is that CobiT was originally constructed primarily as an IT audit tool. Although the move from ISACA to the ITGI sponsorship has broadened its appeal and focus, the heavy IT focus in many of the published CobiT guidance materials scares away some potential users.

The real strength of CobiT is its IT governance focus, as described in Exhibit 5.1. That chart illustrates the importance of the strategic alliance of business and IT resources with value delivery, resource management, risk management, and performance measurement processes. All five of these resources allow an enterprise to establish effective IT governance, and CobiT should help in managing and understanding these concepts. We can expect CobiT published standards and practices to continue to broaden and go beyond just "IT audit" special concepts. All internal auditors should have a CBOK understanding of CobiT and learn to use and understand this internal controls assessment framework.

Notes

1. IT Governance Institute, *CobiT—Governance, Control and Audit for Information and Related Technology*, 4th ed. (Rolling Meadows, IL: 2000).
2. IT Governance Institute, *CobiT 4.1* (Rolling Meadows, IL: 2007).

3. Capability Maturity Model® Integration (CMMi) is a Carnegie Mellon University–developed process improvement approach that provides organizations with the essential elements of effective processes. It can be used to guide process improvement across a project, a division, or an entire organization.
4. IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley,* 2nd ed. (Rolling Meadows, IL: September 2006).
5. IT Governance Institute, *ITAF™: A Professional Practices Framework for IT Assurance* Rolling Meadows, IL: 2008).
6. The IIA definition of internal auditing: www.iia.org.au/pdf/FrequentlyaskedQuestions.pdf.

CHAPTER 6

Risk Management: COSO ERM

Enterprises need to identify all the business risks they face—financial and operational as well as social, ethical, and environmental—and to manage these risks to an acceptable level. Understanding risks is a major component of achieving Sarbanes-Oxley (SOx) compliance, through the Auditing Standard No. 5 (AS 5) Internal audit, in both its assurance and its consulting roles, can contribute to this management of risk. *Risk,* a frequently used term in internal control standards and procedures, has become a term that many internal auditors agree to consider but fail to define. One professional's concept and understanding of risk may be very different from another's, even though they are both working for the same enterprise and in similar areas. This has been particularly true for managers and internal auditors working to improve SOx-related compliance; there has been no consistent understanding of what is meant by the concept of risk.

Particularly to support our understandings of SOx internal controls, internal auditors need to have a better understanding of risk management and how it impacts their skills for building and developing effective internal controls. Chapter 4 on SOx described how the AS 5 external auditing standard introduced risk-based considerations to the process. As discussed, external auditors are required to assess relative risks when selecting the internal accounting control areas to review and consider when performing their reviews.

A major concept behind AS 5 is that management and external auditors should now consider relative risks when implementing and assessing internal controls to achieve compliance with the SOx Section 404 internal control rules. In order to use these new AS 5 auditing standards effectively, all parties should understand the risks surrounding their enterprise and should be able to document and attest to when they did or did not raise an internal controls exception issue, based on relative risks. However, there has been the lack of a consistent definition of what is really meant by *risk*. Although the word has some origins in the insurance industry, *risk* is not consistently used even there.

This all changed when the Committee of Sponsoring Organizations (COSO) released the enterprise risk methodology, COSO Enterprise Risk Management—Integrated Format (COSO ERM). This is an approach that allows an enterprise and internal audit to consider and assess risks at all levels, whether in an individual area, such as for an information technology (IT) development project, or in global risks regarding an international expansion. Released by the same COSO guidance-setting function that has developed and maintains the COSO internal controls framework, COSO ERM sometimes looks like its internal controls brother, but it has a much different feel and approach.

This chapter introduces the COSO ERM framework and its elements, but the emphasis is on why COSO ERM can be an important internal audit tool to better understand and evaluate the risks surrounding internal controls at all levels. We describe major elements of the COSO ERM framework and look at how internal auditors can better build COSO ERM into their audit processes as well as steps for auditing the effectiveness of an enterprise's risk management processes.

An understanding of risk assessment approaches and overall risk management, with an emphasis on COSO ERM should be in every internal auditor's common body of knowledge (CBOK). This chapter discusses risk management fundamentals, introduces COSO ERM, and presents internal audit techniques for understanding and assessing risks in many areas, ranging from selecting areas to review to evaluating risks as part of internal audit reviews. This chapter emphasizes risks on a total enterprise level; Chapter 15 uses some of these same techniques to discuss risk-based audit planning with an emphasis on individual internal audits.

6.1 Risk Management Fundamentals

Every enterprise exists to provide value for its stakeholders, but that value can be eroded through unexpected events at all levels of the enterprise and in all activities, ranging from day-to-day regular operations to setting strategy for some future but uncertain endeavor. All of these activities are subject to uncertainties or risks, whether it is the challenge caused by a new and aggressive competitor or the damage and even loss of life caused by a major weather disturbance. Risk management is an insurance-related concept where an individual or enterprise uses insurance mechanisms to provide protection from those risks. We make these types of decisions based on our assessments of the relative risks and the costs to cover them through the purchase of insurance. Risks and insurance costs also change over time. Fire insurance to cover an individual's home is an example. Back in the days of oil lanterns for light and straw for the horses stored in a nearby stable, there was always a high risk of fires. We only need to think of the great Chicago fire of 1871 where, as legend suggests, a cow kicked over a lantern and caused a fire that devastated the city. The risk of building fires is not that great today, and fire insurance is not that expensive, in a relative sense. However, there is always the possibility that a lightning strike or electrical malfunction will cause a fire in a structure, and mortgage finance companies require fire insurance coverage. Even if no mortgage is held, all prudent persons today purchase such fire insurance even if not required. A destructive fire to one's home presents a low-level but consistent risk. The cost of homeowner fire insurance is relatively low. Individual homeowners might assess other potential risks, such as for earthquakes, and perhaps not purchase insurance for that risk. In a given geographic area, the possibility of an earthquake appears so low that an owner would not consider purchasing any insurance despite the low cost of such a policy. In another situation, an individual may live by a body of water where there are damaging floods every several years. Even if one can purchase flood insurance in such an environment—and most insurance companies will not offer it—the coverage will be very expensive. Some people may decide to accept the risk of a flood in future years and go without insurance coverage. In all of these cases, there has been an insurance purchaser risk management decision.

Starting with these insurance buying foundations, risk management, as it is practiced today, is essentially a post-1960s phenomenon. Moving beyond concerns about natural weather-related events, risk management began to emphasize protecting enterprises against a major catastrophe, such as the risks surrounding a computer system back in the mainframe days, when most information systems assets were stored in one centralized facility. The concern about managing risks surrounding that one centralized computer system moved to a general concern about managing a wide range of other business risks.

Enterprises today face a wide variety of risks and need some tools to sort through all them in order to make rational cost and risk-related decisions. This is the process of risk management. While some in business today just assess an area as high, medium, or low risk and then make quick insurance or risk protection decisions based on those options, others use more sophisticated qualitative or quantitative tools to understand and evaluate risks. The next sections briefly survey some fundamental modern risk management approaches with that aim to help establish more effective enterprise risk management procedures in an enterprise.

An effective risk management process requires four steps: (1) risk identification, (2) quantitative or qualitative assessment of the documented risks, (3) risk prioritization and response planning, and (4) risk monitoring. There is always a need to identify and understand the various risks facing an enterprise, to assess those risks in terms of their cost or impact and probability, to develop responses in the event of a risk occurrence, and to develop documentation procedures to describe what happened as well as corrective actions going forward. The same is true for enterprise-wide risk management decisions and for the decisions of an internal auditor in the course of a single review engagement. This section focuses on the management of risks across an enterprise. Chapter 15 uses some of these same concepts when doing risk-based internal audit planning.

This four-step risk management process should be implemented at all levels of the enterprise and with the participation of many different people. Whether a small enterprise operating in a limited geographic area or a larger, worldwide enterprise, risk management approaches should be developed for the total enterprise. This is particularly important for the worldwide enterprise with multiple operating units engaged in different business operations and with facilities in different countries. Some risks in one unit may directly impact or be related to risks in another, but other risk considerations may be effectively independent from the whole. These common risks can occur because of a wide variety of circumstances ranging from poor financial decisions, to changes in consumer tastes, to new government regulations.

(a) Risk Identification

Management should endeavor to identify all possible risks that may impact the success of the enterprise, ranging from the larger or more significant overall business risks down to the less important risks associated with individual projects or smaller business units. The risk identification process requires a studied, deliberate approach to looking at potential risks in each area of operations and then identifying the more significant risk areas that may impact each operation in a reasonable time period. The idea here is not just to list every possible risk but for an enterprise to identify those that might have a more major impact operations, within a reasonable time period. This can be a difficult exercise because we can only estimate the probability

of the risk occurring or the nature of the consequences if the enterprise has to face the risk. This risk identification process should occur at multiple levels with an understanding that a risk that impacts an individual business unit or project may not have that great an impact on the entire enterprise or beyond. Conversely, a major risk that impacts the entire economy will flow down to the individual enterprise and its separate business units. Some major risks are so infrequent but still can be so cataclysmic that it is difficult to identify them as possible future events.

A good way to start the risk identification process is with a high-level organization chart listing corporate-level as well as operating units. Each of those units may have facilities in multiple global locations and may consist of multiple and different types of operations. Each separate facility will then have its own departments or functions. Some of these separate facilities may be closely connected to one another; others may represent little more than corporate investments. A difficult and sometimes complicated task for a larger enterprise, an initiative should be launched to identify all risks in various individual areas. This type of exercise can result in interesting and/or sometimes troubling results. For example, a corporate-level senior manager may be aware of some product liability risks but a front-line supervisor in an operating unit may look at the same risks with an entirely different perspective.

A marketing manager may be concerned about a competitor's pricing strategies or the risk of pricing activities that would put the enterprise in violation of restraint of trade laws. An IT manager may be concerned about the risk of a computer virus attack on application systems but will have little knowledge of the pricing issue risks. More senior management typically will be aware of a different level and set of risks than would be on the minds of the operations-oriented staff. Still, all of these risks should be identified and considered on an operating unit–by–unit basis and over the entire enterprise.

To be effective, this risk identification process requires much more than just sending out an e-mail to all operating units with a request for recipients to list key risks in their operating units. Such a request typically results in a wide range of inconsistent answers with no common approach. A better approach is to identify people at all levels of the enterprise to serve as risk assessors. Within each significant operating unit, key people should be identified from operations, finance/accounting, IT, and unit management. Their goal would be to identify and then help assess risks in their units built around a risk identification model framework. This type of initiative can be led by the chief executive officer (CEO) and an enterprise risk management group, if one exists, or a function such as internal audit.

The whole idea here is to outline some high-level "straw man" risks that may impact various operating units. Knowledgeable people can then look at these lists and expand or modify them as appropriate. Exhibit 6.1 shows some types of major risks that may impact an enterprise, including various strategic, operations, and finance risks. This is the type of high-level list that a CEO might use to a common shareholder annual meeting question "What worries you at the end of the day?" Although it does not list all of the risks facing the enterprise, this first-pass list can be used to get started on a detailed identification of risks. Enterprise senior management—often the CEO and supporting staff—can meet to ask some of these "What worries you. . ." types of questions to identify these risks.

EXHIBIT 6.1 Types of Enterprise Risks

Enterprise-Wide Strategic Risks

External Factors Risks
- Industry Risk
- Economy Risk
- Competitor Risk
- Legal and Regulatory Change Risk
- Customer Needs and Wants Risk

Internal Factors Risks
- Reputation Risk
- Strategic Focus Risk
- Parent Company Support Risk
- Patent/Trademark Protection Risk

Operations Risks

Process Risks
- Supply Chain Risk
- Customer Satisfaction Risk
- Cycle Time Risk
- Process Execution Risk

Compliance Risks
- Environmental Risk
- Regulatory Risk
- Policy and Procedures Risk
- Litigation Risk

People Risks
- Human Resources Risk
- Employee Turnover Risk
- Performance Incentive Risk
- Training Risk

Finance Risks

Treasury Risks
- Interest Rate Risk
- Foreign Exchange Risk
- Capital Availability Risk

Credit Risks
- Capacity Risk
- Collateral Risk
- Concentration Risk
- Default Risk
- Settlement Risk

Trading Risks
- Commodity Price Risk
- Duration Risk
- Measurement Risk

Information Risks

Financial Risks
- Accounting Standards Risk
- Budgeting Risk
- Financial Reporting Risk
- Taxation Risk
- Regulatory Reporting Risk

Operational Risks
- Pricing Risk
- Performance Measurement Risk
- Employee Safety Risk

Technological Risks
- Information Access Risk
- Business Continuity Risk
- Availability Risk
- Infrastructure Risk

This very general, high-level risk model can serve as a basis to better define the specific risks facing various units an enterprise, such as the entry in this exhibit of business continuity risks under technological risks. An IT manager should be able to expand this to a long list of detailed technology-related risks associated with business continuity. An operations manager who is the user of IT resources might look at business continuity risks from a different perspective and may introduce other new risks associated with what happens if IT services are not available. In order to have a better understanding of the risks facing an enterprise, it is often best to expand these lists to establish a more complete set of risks.

An enterprise management team should then start with this more complete list of potential enterprise risks and ask themselves questions along the lines of:

- Is the risk common across the overall enterprise or unique to one business group?
- Will the enterprise face this risk because of internal or through external events?
- Are the risks related, such that one risk may cause another to occur?

The idea is to gain a strong understanding of the nature of enterprise-level risks and then to highlight the major risks, such as the risk of a significant fall in customer satisfaction ratings, the risk of a new and very large competitor entering the market, or the risk of an identified significant control weakness as part of the financial statement close. Any of these major risks could present significant challenges to the enterprise.

Enterprise management should review these identified risks and highlight those that appear to be most critical to the enterprise. Then it should prepare a final set of identified organization risks by the overall enterprise and by specific operating units. Because viewpoints and perspectives will vary across the enterprise, these identified risks should be shared with responsible operating and financial management, giving them opportunities to provide feedback. The idea here is to identify the population of risks that threaten an enterprise, both at an individual unit level and on a total corporate basis. These will not necessarily become the core risks but often are a starting point for enterprise risk assessments.

(b) Key Risk Assessments

Having identified the significant enterprise risks, a next step is to assess their likelihood and relative significance. A variety of approaches can be used here, ranging from best-guess qualitative approaches to some detailed, very mathematical quantitative analyses. The idea is to help decide which of a series of potentially risky events should give management the most to worry about. Responsible managers should assess these risks using a questionnaire approach:

- What is the likelihood of this risk occurring over the next one-year period? Using a score of 1 to 9, assign a best-guess score as follows:
  - Score 1 if you see *almost no chance* of that risk happening during the period.
  - Score 9 if you feel the event will *almost certainly happen* during the period.
  - Score 2 through 8 depending on how you feel the likelihood fall between these two ranges.
- What is the significance of the risk in terms of cost to the overall enterprise? Again using a 1 to 9 scale, scoring ranges should be set depending on the financial significant of the risk. A risk whose costs could lower earnings per share by perhaps 1 cent might qualify for the maximum score of 9.

These questionnaires should be independently circulated to knowledgeable people to score each of the identified risks for these two measures. As an example, assume that an enterprise has identified six risks, R-1 through R-6, and four managers are asked to separately evaluate each risk in terms of likelihood and significance. These scores can then be averaged by both factors and plotted on a risk assessment

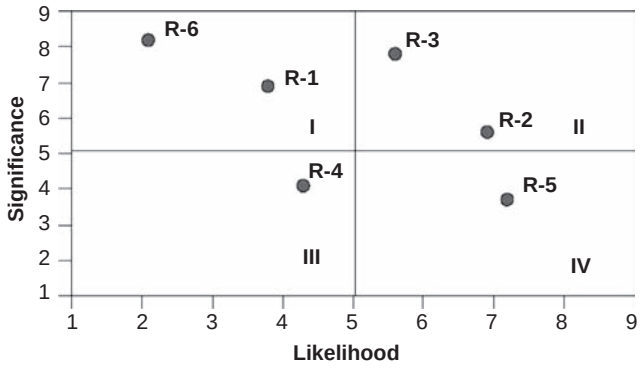


EXHIBIT 6.2 Risk Assessment Analysis Map

Source: COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework, Robert R. Moeller, Copyright © 2007 John Wiley & Sons. Reprinted with the permission of John Wiley & Sons, Inc.

analysis chart as shown in Exhibit 6.2. R-1 had an average likelihood score of about 3.75 and a significance score of 7.00, and this score is plotted in quadrant I of the example chart. For example, the chart shows R-1 as a relatively significant but not that likely to occur. With all identified risks plotted in this manner, the high likelihood and more significant risks in quadrant II should receive immediate management attention. This type of risk assessment analysis chart provides a good qualitative measure to understand significant risks surrounding an enterprise.

This high-risk assessment process works quite well when an enterprise has identified a relatively small number of risks. It is fairly easy to look at the analysis chart and focus on remediation planning for the high-likelihood and significant risks in the upper left-hand quadrant. Often, however, an enterprise may have identified a much larger set of risks, and ranges of only 1 to 9 and plots on the example chart will not provide sufficient detail. A sometimes better approach is to express these significance and impact estimates in terms of a two-digit percentage estimate (e.g., 72%) of achieving some risk or as a probability (e.g., 0.72). However, just increasing the number of digits, from a 7 to a full 72%, does not increase the accuracy of the assessment. More attention should be given to better understanding the relationship between probabilities covering independent and related risk events.

(i) PROBABILITY AND UNCERTAINTY When a large number of risks have been identified, management should think of the individual estimated risk likelihoods and occurrences in terms of two-digit probabilities ranging from 0.01 to 0.99. We have used this range because risks never have a zero chance or 100% chance of occurring; otherwise they would not be risks. A basic rule of probability is that we cannot add up independent probability estimates to yield a joint estimate. If the probability of risk A occurring is 60% and the probability of a separate but related risk B is also 60%, we can *not* say that the probability of both occurring is 0.60 + 0.60 = 1.20. This 120% does not make sense. Rather, the joint probability of two independent events is the product of the two separate probabilities. That is:

$$\Pr(\text{Event 1}) \times \Pr(\text{Event 2}) = \Pr(\text{Both Events})$$

That is, if Event 1 is 0.60 and Event 2 also 0.60, the combined probability of both events occurring is (0.60) × (0.60) = 0.36. In terms of the assessments, if a risk has a 60% significance estimate or we are 60% certain that the risk will occur and if the impact has been rated at 60%, there is a 36% probability that we will achieve both of those risks. We can also call this the risk score for the individual risk.

An accurate risk assessment process, however, requires more than just top-of-the-head estimates, whether stated in a single 1 to 9 range or as a full two-digit percentage. Enterprise management should take a hard look at identified risks and gather more information, if required. For example, during the risk identification process, one manager may have identified the consequences of a new tariff law as a serious risk. However, responsible managers may want to better understand its actual consequences. It may be something that is not applicable to the unit in question or that does not go into effect until some years in to the future. The point here is that some additional information may be needed before all identified risks can be accurately assessed.

(ii) RISK INTERDEPENDENCIES We have discussed risks at an individual organizational unit level, but risk independencies must always be considered and evaluated throughout the organizational structure. Although an entity should be concerned about risks at all levels of the organization, it really has control over only those risks within its own sphere. The 2002 example of the fall of the public accounting firm Arthur Andersen in the wake of the Enron collapse is an example. Each city-by-city and country-by-country unit of that public accounting firm had its own risk assessment procedures, following firm-wide standards. However, a risk event at one operating office, Houston, caused the worldwide firm to collapse. An operating office in another area, such as Toronto, might not have fully anticipated such risks in faraway Houston. The point is that risks are often very interdependent within an enterprise. Each operating unit is responsible for managing its own risks but may be subject to the consequences of risk events on units above or below it in the organization structure.

(iii) RISK RANKING Although the examples in this chapter show a short list of identified risks, a typical enterprise will end up with a very long list of potential risks. A next step is to take the established significance and likelihood estimate, calculate risk rankings, and identify the most significant risks across the entity reviewed. Exhibit 6.3 is an example of this type of analysis. Based on the likelihood and significance scores from Exhibit 6.2, the product of these two gives relative risk rankings. Risks C and G have the highest risk rank scores and would be plotted in the upper right-hand quadrant as the most significant risks in this sample. These two are often called the risk drivers or the primary risks for this set of identified risks. An organization should then focus its attention going forward on these primary risks. These risk-ranked schedules should be organized on a unit-by-unit basis and adjusted to accommodate all related risks in parallel with as well as above or below the entity being ranked or evaluated.

Management must identify these unit-by-unit assessed risks to make certain that risk likelihood and significance estimates are appropriate throughout. All too often, risk events that occur far away from corporate headquarter offices cause major problems. An example from over 20 years ago can be drawn from a risk event at the once-major U.S. corporation, Union Carbide. On the night of December 2, 1984,

EXHIBIT 6.3 Risk Scoring Schedule

Identified Risk	Significance Probability	Likelihood Probability	Risk Score (P × I)	Rank
A	0.55	0.30	0.17	8
B	0.88	0.24	0.21	7
C	0.79	0.66	0.52	1
D	0.77	0.45	0.35	4
E	0.35	0.88	0.31	5
F	0.54	0.49	0.26	6
G	0.62	0.72	0.45	2
H	0.66	0.20	0.13	9
I	0.90	0.45	0.41	3
J	0.12	0.88	0.11	10

over 40 tons of poisonous gases leaked from a pesticide factory owned by Union Carbide in Bhopal, India, killing more than 20,000 residents.[1] After much legal wrangling, Union Carbide, which had built that plant in 1969, settled a civil suit brought by the Indian government in 1989 by agreeing to pay $470 million for damages suffered by the half million people who were exposed to the gas. The company maintained that the payment was made out of a sense of "moral" rather than any "legal" responsibility since the plant was operated by a separate Indian subsidiary, Union Carbide India Limited (UCIL), but court proceedings revealed that management's cost-cutting measures had effectively disabled safety procedures essential to prevent or alert employees of such disasters. Dow Chemical has since taken over Union Carbide and denies responsibility for this disaster. However, because of the tremendous loss of life there and because Dow is much larger than what was Union Carbide and its UCIL subsidiary, ongoing litigation continues to haunt Dow.

The Bhopal gas leak is an example of how a risk event at a distant and relatively small unit can have disastrous consequences on a major corporation. While the risk identification and assessment rules outlined in this chapter would not have accounted for this magnitude of a catastrophe, and each unit in an enterprise needs to recognize the likelihoods and consequences of risks at individual unit levels, a risk event at a small foreign subsidiary can bring down the entire enterprise. Risk management at all levels should recognize that catastrophes can happen. Although we never can predict risks of this major consequence; an enterprise should always be aware of the worst disaster that can happen.

(c) Quantitative Risk Analysis

(i) EXPECTED VALUES AND RESPONSE PLANNING There is little value in identifying significant risks unless an enterprise has at least some preliminary plans for the actions necessary if one of the risks occurs. The idea is to estimate the cost impact of incurring some identified risk and then to apply that cost to a risk factor probability to derive an expected value or cost of the risk. Often this exercise does not require detailed cost studies with lots of supporting historical trends and estimates. Rather, expected cost estimates should be performed by front-line people at various levels of the enterprise who have knowledge of the area or risk implications.

The idea is to go through each of the identified risks—or only the key risks if time is limited—and estimate the costs of incurring the risk. Because these kinds of risks involve such matters as the failure of a hardware component, the drop in market share, or the impact of a new government regulation, typically these costs cannot just be looked up in a current vendor catalog. Some typical risks, labeled A, B, and C, illustrate this type of thinking:

Risk A: Loss of up to x% market share due to changing consumer tastes.
- Estimate the reduction in sales and loss of profits due to the x% drop.
- Estimate much will it cost to begin to restore the lost market position.

Risk B: Temporary loss of major manufacturing facility for zz days due to a hurricane severe weather event.
- Estimate the best- and worst-case costs to get the plant temporarily repaired and back in operation within zz days.
- Estimate the extra labor and production costs incurred during the interim.

Risk C: Loss of IT systems for two days due to pernicious computer virus.
- Estimate the business and profitability loss during the down period.
- Estimate the cost to transfer operations to the business continuity site.

These factors illustrate the type of thinking needed to estimate the costs of recovering from some risk event. It is often difficult to determine what it would cost to recover from these risks. While there is no need to perform detailed, time-consuming analyses here, knowledgeable people who understand the risk area often can provide good estimates by considering questions of this type:

1. What is the best-case cost estimate of incurring the risk? This is an assumption that there will be only limited impact if the risk occurs.
2. What would a sample of knowledgeable people estimate for the cost? For Risk A as outlined, the director of marketing might be asked to supply an estimate.
3. What is the expected value or cost of incurring the risk? This is the type of risk that might include some base costs as well as such other factors as additional labor requirements.
4. What is the worst-case cost of incurring the risk? This is a what-if-everything-goes-wrong type of estimate.

We have suggested using four estimates as an idea of the ranges of costs in various people's thinking. However, one best-guess estimate should be selected from the four estimates—usually something between estimates 2 and 3 in the list. These estimates and supporting work should be documented, with the selected cost estimate entered as the cost impact on Exhibit 6.4, the risk response planning schedule. These are the same risks that were identified in the Exhibit 6.3 schedules but here are ordered by risk rank. This reordering is important when an enterprise has a long list of identified risks.

The expected value or cost values in Exhibit 6.4 are just the products of the cost impacts and their risk scores. This is an estimate of what it will cost an enterprise to incur some risk. Although the numbers selected for these samples are very arbitrary, they show how a risk management specialist should interpret or act on this type of analysis. Risk C, for example, has a high likelihood and significance as well as fairly high expected cost to correct. This is the type of risk that management

EXHIBIT 6.4 Risk Ranking Expected Cost Example

Identified Risk	Significance Probability	Likelihood Probability	Risk Score (P × I)	Rankings	Cost Impact	Expect Cost (Cost × Score)
C	0.79	0.66	0.52	1	$120,600	$62,881
G	0.62	0.72	0.45	2	$785,000	$350,424
I	0.90	0.45	0.41	3	$15,000	$6,075
D	0.77	0.45	0.35	4	$27,250	$9,442
E	0.35	0.88	0.31	5	$52,350	$16,124
F	0.54	0.49	0.26	6	$1,200	$318
B	0.88	0.24	0.21	7	$12,650	$2,672
A	0.55	0.30	0.17	8	$98,660	$16,279
H	0.66	0.20	0.13	9	$1,200,980	$158,529
J	0.12	0.88	0.11	10	$88,600	$9,356

should identify as a candidate for corrective actions. However, the next risk on the schedule, Risk G, also belongs in the upper left-hand side of the quadrant but with a relatively low cost to implement. Management may decide to accept this risk or to develop some other form of remediation plan. Risk H is another with a high cost to implement risk, fairly high significance, and a low likelihood of occurrence. Often for these types of risks, management may decide to hope for the best and live with them. Such risks are expensive if incurred but also expensive to protect against.

(ii) RISK MONITORING The identification of key risks can never be a single, one-time process. The environments surrounding identified risks will soon change as surrounding conditions change. For some risks, conditions may change such that the risk becomes an even greater threat. For example, management may have identified potential political risks in some less-developed country, but events often happen quickly, and political changes in that same country can make those concerns even riskier. An enterprise needs a mechanism to monitor these identified risks.

Risk identification processes are not continuous exercises. Just as an enterprise will prepare an annual budget with revisions perhaps once per quarter, a risk identification process is often an annual or quarterly process. Once these risks have been identified, the enterprise needs to monitor them and make ongoing adjustments as needed. This risk monitoring can be performed by the process owner or by an independent reviewer. Internal audit often is a very credible and good source to monitor the current status of identified risks. It may gather this information through surveys or face-to-face reviews. Internal audit always has a level of extra credibility and authority. When the auditors ask about the status of some identified risk area, those responsible for the area will quite probably provide accurate information. If internal audit is unable to acquire good information regarding the status of some identified risk, it can always schedule a visit to better understand the nature of the risk area. Of course, internal auditors have their own audit project scheduling and risk assessment issues; they typically cannot just schedule a review in a short time frame to understand the current status of some identified risk. However, if people in the enterprise know that internal auditors sometimes may visit to better understand the status or some risk, there will be a strong tendency to provide some strong, accurate status answers.

Accurate monitoring processes are an essential component of risk management. An enterprise may have gone through an elaborate process to identify its more significant risks. However, the current status of those risks needs to be monitored on a regular basis with changes made to the identified risks as necessary.

6.2 COSO ERM: Enterprise Risk Management

COSO Enterprise Risk Management is a framework to help enterprises to have a consistent definition of their risks. It is also an important tool for understanding and improving SOx internal controls. COSO ERM was launched in manner similar to the development of the COSO internal control framework, as discussed in Chapter 3. Just as there was no consistent definition of *internal controls,* there was also no consistent enterprise-level definition of *risk.* This concern was emphasized by the comments of John Flaherty, the first chairman of COSO: "Although a lot of people are talking about risk, there is no commonly accepted definition of *risk management* and no comprehensive framework outlining how the process should work, making risk communication among board members and management difficult and frustrating."[2] COSO contracted with PricewaterhouseCoopers (PwC) to develop this risk framework. The COSO ERM framework was published after the enactment of SOx in September 2004. The remainder of this chapter summarizes COSO ERM in some detail.

Just as the COSO internal controls framework started by proposing a consistent definition of its subject, the COSO ERM framework document starts by defining enterprise risk management:

> *Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*

Professionals should consider the key points supporting this COSO ERM framework definition including:

- **ERM is a process.** An often misused expression, the dictionary definition of a *process* is a set of actions designed to achieve a result. However, this definition does not provide much help for many professionals. The idea here is that a process is not a static procedure, such as the use of an employee badge designed and built to allow only certain authorized persons to enter a locked facility. Such a badge procedure—like a key to a lock—only either allows or does not allow someone entry to the facility. A process tends to be a more flexible arrangement. In a credit approval process, for example, acceptance rules are established with options to alter them given other considerations. An enterprise might bend the credit rules for an otherwise good credit customer that is experiencing a short-term problem. ERM is that type of a process. An enterprise often cannot define its risk management rules through a small, tightly organized rule book. Rather there should be a series of documented steps to review and evaluate potential risks and to take action based on a wide range of factors across the entire enterprise.

- **ERM process is implemented by people in the enterprise.** An ERM will not be effective if it is implemented only through a set of rules sent into an operating unit from a distant corporate headquarters, where those corporate people who drafted the rules may have little understanding of the various decision factors surrounding the operating units. The risk management process must be managed by people who are close enough to that risk situation to understand the various factors surrounding the risk, including its implications.
- **ERM is applied through the setting of strategies across the overall enterprise.** Every enterprise is constantly faced with alternative strategies regarding a vast range of potential future actions. Should the entity acquire another complementary business to expand growth or just build internally? Should it adopt a new technology in manufacturing processes or stick with the tried and true? An effective ERM set of processes should play a major role in helping to establish those alternative strategies. Since many enterprises are large with many different operating units, ERM should be applied across the entire enterprise using a portfolio type of approach that blends a mix of high- and low-risk activities.
- **Concept of risk appetite must be considered.** A new concept or term for many, *risk appetite* is the amount of risk, on a broad level, that an enterprise and its individual managers are willing to accept in their pursuit of value. Risk appetite can be measured in a qualitative sense by looking at risks in such categories as high, medium, or low; alternatively, it can be defined in a qualitative manner. An understanding of risk appetite covers a wide variety of issues that are discussed further in this chapter as part of implementing COSO ERM to strengthen an enterprise's SOx internal controls environment. The basic idea is that every manager and, collectively, every enterprise have some appetite for risk. Some will accept risky ventures that promise potentially high returns; others prefer a more guaranteed-return, low-risk approach. This appetite for risk concept can be considered in terms of two investors. One may prefer to invest in very low risk but typically low-return money market or index funds while another may invest in low-cap start-up technology stocks with expectations of very high returns. That latter investor can be described as having a high appetite for risk. As another example, on a street intersection with a Walk or Don't Walk crossing light, the person who keeps crossing the intersection when the light begins to flash "Walk," meaning it will soon change to "Don't Walk," has a higher appetite for risk.
- **ERM provides reasonable but not positive assurance on objective achievements.** The idea here is that an ERM, no matter how well thought out or implemented, cannot provide management or others with any assured guarantee of outcomes. A well-controlled enterprise, with people at all levels consistently working toward understood and achievable goals, may achieve those objectives period after period, even over multiple years. However, an unintentional human error, an unexpected action by another, or even a natural disaster can occur. Despite an effective ERM process, an enterprise can experience a major and totally unexpected catastrophic event. Reasonable assurance does not provide absolute assurance.
- **ERM is designed to help achieve objectives.** An enterprise, through its management, should work to establish high-level common objectives that can be shared by all stakeholders. Examples here, as cited in the COSO ERM published

documentation, include such matters as achieving and maintaining a positive reputation within an enterprise's business and consumer communities, providing reliable financial reporting to all stakeholders, and operating in compliance with laws and regulations. The overall ERM program for an enterprise should help it to achieve those objectives.

ERM-related goals and objectives are of little value unless they can be organized and modeled together in a manner that management can look at the various aspects of a task and understand—at least sort of—how they interact and relate in a multidimensional manner. This is a real strength of the COSO internal control framework model. It describes, for example, how an enterprise's compliance with regulations impacts all levels of internal controls, from monitoring processes to the control environment, and how that compliance is important for all entities or units of the enterprise. The COSO ERM framework provides some common definitions of risk management and can help to achieve SOx internal control objectives as well as better risk management processes throughout the enterprise.

6.3 COSO ERM Key Elements

The COSO internal control framework, as shown in Exhibit 3.1, has become a worldwide model for describing and defining internal controls and has been the basis for establishing SOx Section 404 compliance. Perhaps because some of the same team members were involved with COSO internal controls and ERM, the COSO ERM framework[3] —at first observation—looks very similar to the COSO internal controls framework. Exhibit 6.5 shows this COSO ERM framework as a three-dimensional

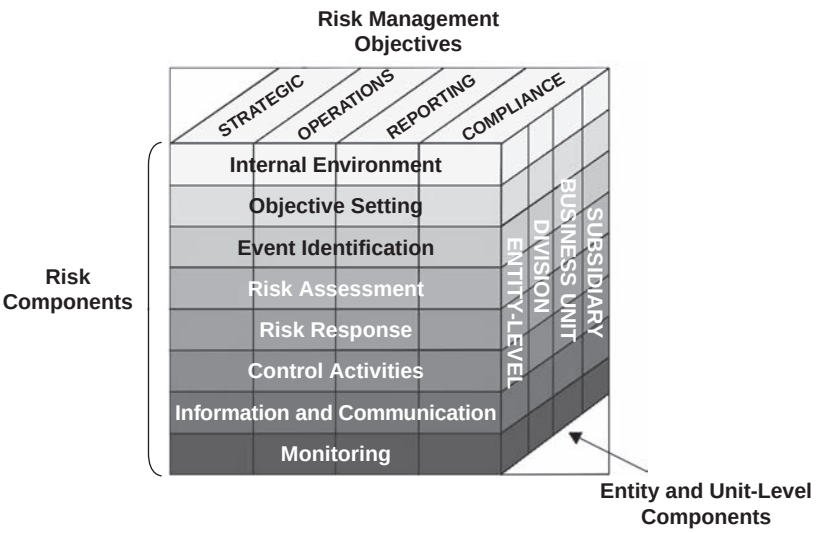


EXHIBIT 6.5 COSO ERM Framework

Source: COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework, Robert R. Moeller, Copyright © 2007 John Wiley & Sons. Reprinted with the permission of John Wiley & Sons, Inc.

cube with the components of:

- Four vertical columns representing the strategic objectives of enterprise risk.
- Eight horizontal rows or risk components.
- Multiple levels to describe any enterprise, from a "headquarters" entity level to individual subsidiaries. Depending on organization size, there can be many slices of the model here.

This section describes the horizontal components of COSO ERM; later sections discuss its other two dimensions and how they all relate to one another. The aim of this ERM framework is to provide a model for enterprises to consider and understand their risk-related activities at all levels as well as how these risk components impact one another. An objective of this chapter is to help internal auditors—from the chief audit executive (CAE) to staff auditors—to better understand COSO ERM and learn how it can help manage a wide range of risks facing enterprises.

Because the COSO ERM framework diagram looks very similar to the COSO internal controls framework that has become familiar to many internal auditors over recent years and certainly after SOx, some have sometimes incorrectly viewed COSO ERM as just a new update to the COSO internal controls framework. However, COSO ERM has different objectives and uses. *COSO ERM should not be considered just a new and improved or revised version of the COSO internal control framework.* It is much more. The next sections outline this framework from a risk components perspective.

(a) Internal Environment Component

Looking at the face of the COSO ERM cube, there are eight levels, with the internal environment located at the top of ERM framework. In contrast, in the COSO internal control framework, the control environment factor placed at the foundation level. The internal environment may be thought of as the capstone to COSO ERM. This component is similar to the box at the top of an organizational chart that lists the CEO as the designated head of a function. This level defines the basis for all other components in an enterprise's ERM model, influencing how strategies and objectives should be established, how risk-related business activities are structured, and how risks are identified and acted on. While the COSO internal controls control environment focuses on current practices in place, such as human resources policies, ERM takes a more future-directed, philosophy-oriented approach. The COSO ERM internal environment component consists of these elements:

- **Risk management philosophy.** These are the shared attitudes and beliefs that characterize how the enterprise considers risk in everything it does. More than a message in a code of conduct, a risk management philosophy is the attitude that should allow stakeholders at all levels to respond to high-risk proposals with an answer along the lines of perhaps "No, that is not the kind of venture our company will be interested in." Of course, an enterprise with a different philosophy might respond to this same proposal with "Sounds interesting. What's the expected rate of return?" Neither response is really wrong, but an enterprise should try to develop a consistent attitude to how it accepts risky ventures.

This risk philosophy is important when internal auditors evaluate SOx internal controls.

- **Risk appetite.** Appetite is the amount of risk an enterprise is willing to accept in the pursuit of its objectives. An appetite for risk can be measured in quantitative or qualitative terms, but all levels of management should have a general understanding of their enterprise's overall risk appetite. The term *appetite* was not used often by internal auditors and other managers prior to COSO ERM, but it is a useful expression that describes an overall risk philosophy.
- **Board of directors attitudes.** The board and its committees have a very important role in overseeing and guiding an enterprise's risk environment. The independent, outside directors in particular should closely review management actions, ask appropriate questions, and serve as a check-and-balance control for the enterprise. When a senior enterprise officer has an it-can't-happen-here attitude regarding possible risks at various levels, members of the board should ask hard questions about how the enterprise would react if one of those events actually does happen.
- **Integrity and ethical values.** This important ERM internal environment element requires more than just a published code of conduct and includes a well-thought-out mission statement and integrity standards. These materials help to build a strong culture to guide the enterprise, at all levels, in helping to make risk-based decisions. Stronger ethical values here might have helped enterprises, such as Enron and WorldCom, to avoid the accounting scandals that led to the enactment of SOx. This area should be an essential component in every ERM framework today.
- **Commitment to competence.** *Competence* refers to the knowledge and skills necessary to perform assigned tasks. Management decides how these critical tasks will be accomplished through developing strategies and assigning the proper people to perform them. We have all seen enterprises that do not have this type of commitment. Senior management sometimes makes grand and loud plans to accomplish some goal but then does little to achieve it. The stock market frequently punishes failures in such activities. With a strong commitment to competence, managers at all levels should take steps to achieve their promised goals.
- **Organizational structure.** An enterprise should develop an organizational structure with clear lines of authority, responsibility, and appropriate reporting. Every professional has seen situations where an organization does have appropriate lines of communication. For example, prior to SOx, many internal audit functions had published organizational charts showing them reporting to their board audit committees, but often that was only on paper; there were limited internal audit day-to-day communications beyond periodic, very brief audit committee meetings. SOx has changed this. Those environments where the audit committee had only very limited interaction with its internal audit function represented a failure in organizational structure. While this situation has been corrected, many situations organizational structure may need improvement to achieve effective ERM.
- **Assignments of authority and responsibility.** This ERM component refers to the extent to which authority and responsibility is assigned or delegated. The trend in many enterprises today is to push approval authority responsibilities down the organizational chart, giving lower-level and even first-line employees

greater authorization and approval authority. A related trend has been to flatten organizations by eliminating middle management levels. These structures usually encourage employee creativity, faster response times, and greater customer satisfaction. However, this type of customer-facing organization requires strong procedures and rules for the staff as well as management so that lower-level staff decisions can be overruled if necessary. All individuals should know how their actions interrelate and contribute to the overall objectives of the enterprise. A strong code of conduct is a critical element here.

- **Human resource standards.** Practices regarding employee hiring, training, compensating, promoting, disciplining, and all other actions send messages regarding what is favored, tolerated, and forbidden. When management winks at or ignores some gray-area activities rather than taking a strong stand, that message usually is informally and quickly communicated to others. Strong standards are needed to ensure that human resource rules are both communicated to all stakeholders and enforced.

The published COSO ERM guidance materials contain other examples of the components necessary to build an effective internal environment. Many refer to the standards and approaches an enterprise should implement to accept and manage various levels of risk, and others refer to just good business practices. No matter whether an enterprise has a high or low appetite for risk, it needs to establish control environment practices to manage those risks. For example, the enterprise can give its sales force a rather free rein to do deals without much management supervision and approval. Yet everyone should know the legal, ethical, and management policy limits of those free-rein practices. Processes should be in place such that if anyone steps over the line regarding these limits, swift remedial actions are taken and communicated. There are many ways for an enterprise to communicate its risk management standards, but a formal statement in the annual report or information on the enterprise's Web home page are often good places.

Two internal environment components of COSO ERM, the enterprise's risk management philosophy and its relative appetite for risk, feed other elements of the COSO ERM framework. While risk management philosophy was discussed in terms of board of directors' attitudes and human resource policies, among others, risk appetite is often a softer measure, where an enterprise has determined that it will accept some risks but reject others in terms of their likelihood and impact. Exhibit 6.6 shows a risk appetite map. An enterprise should recognize the range in which it is willing to accept risks in terms of their likelihood and impact. This exhibit says that an enterprise may be willing to get involved in a high-negative-impact project if there is a low likelihood of an occurrence. There is a third dimension to this chart as well. An enterprise will sometimes have a greater appetite for a more risky endeavor if there is a higher potential return.

(b) Objective Setting

Ranked right below the internal environment in the COSO ERM framework, objective setting outlines important conditions to help management create an effective ERM process. This element says that, in addition to an effective internal environment, an enterprise must establish a series of strategic objectives, aligned with its mission and covering operations, reporting, and compliance activities. COSO ERM

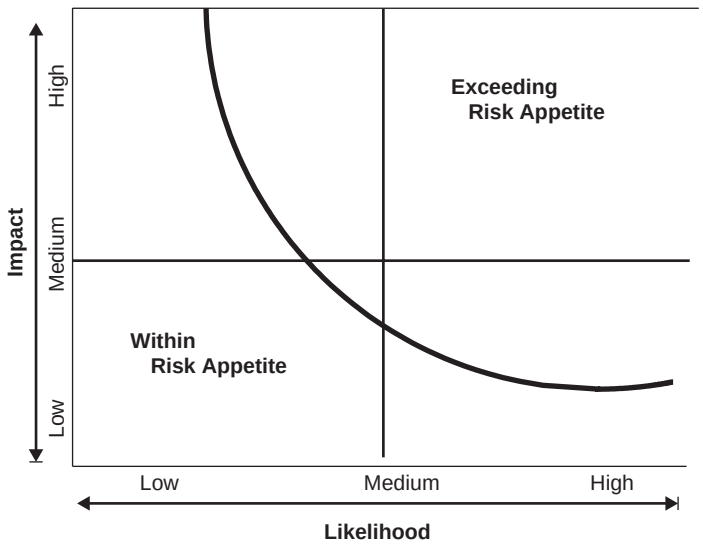


EXHIBIT 6.6 Risk Appetite Map

Source: COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework, Robert R. Moeller, Copyright © 2007 John Wiley & Sons. Reprinted with the permission of John Wiley & Sons, Inc.

emphasizes that a mission statement is a crucial element for setting objectives; it is a general, formalized statement of purpose and a building block for the development of specific functional strategies. Often just a simple, straightforward statement, a mission statement should summarize an enterprise's objectives and its overall attitude toward risks. Properly done and delivered, a mission statement should encourage an enterprise to develop high-level strategic objectives and then to help select and implement operations, reporting, and compliance objectives. While operations objectives pertain to the effectiveness and efficiency of the enterprise in achieving profitability and performance, compliance goals cover the reporting of performance and compliance with laws and regulations. COSO ERM calls for an enterprise to formally define its goals with a direct linkage to its mission statement, along with measurement criteria to assess if it is achieving these risk management objectives.

The ERM internal environment component of understanding the enterprise's risk management philosophy and risk appetite calls for the objective-setting component to formally define that risk appetite in terms of a tolerance for risk. Tolerances are guidelines that an enterprise should use—at all levels—to assess whether it will accept risks. Establishing and enforcing risk tolerances can be very difficult, with potential problems if these rules are not clearly defined, well understood, and strictly enforced. An enterprise should establish tolerable ranges of acceptable risks in many areas. For example, products coming off production lines might have acceptable preestablished error rates of less than some value, such as an error rate no greater than 0.005%. That is an acceptably low error rate in many areas, and production management here would accept the risk of any product warranty claims or damage to their reputation if there were errors within that relatively narrow limit. Of course,

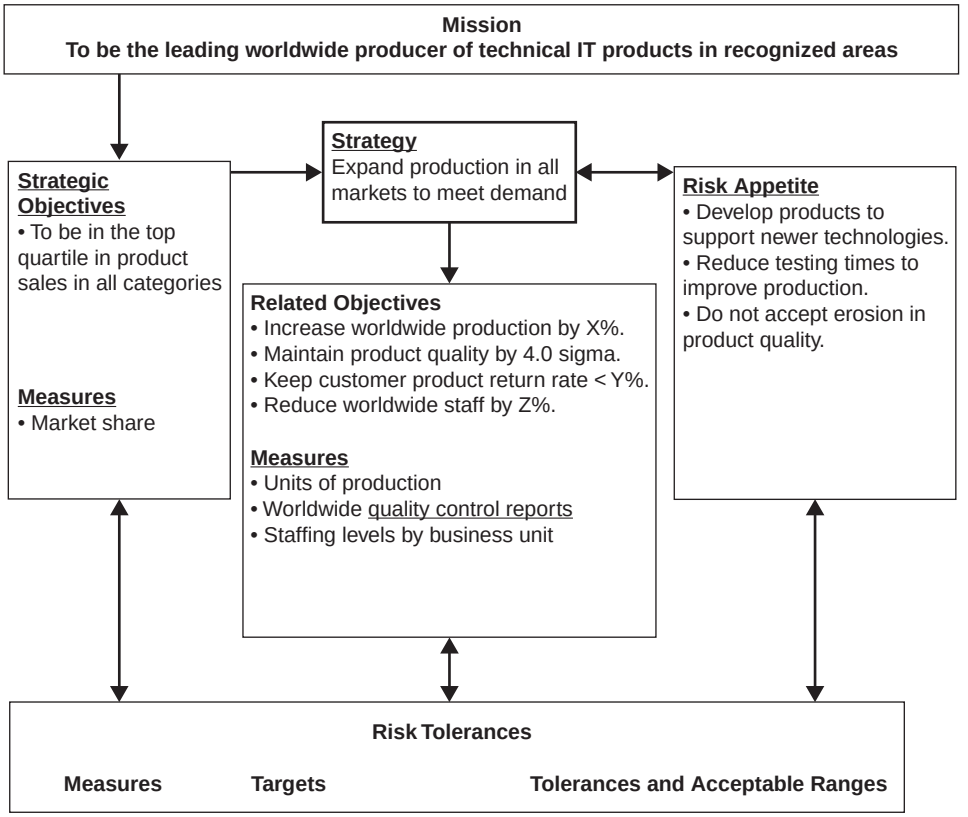


EXHIBIT 6.7 COSO ERM Objective-Setting Components

Source: COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework, Robert R. Moeller, Copyright © 2007 John Wiley & Sons. Reprinted with the permission of John Wiley & Sons, Inc.

today's quality assurance emphasis on six sigma programs, discussed in Chapter 32, brings those tolerance limits much tighter.[4]

The point here is that an enterprise should define its risk-related strategies and objectives. Within those guidelines, it should decide on its appetite and tolerance for these risks. That is, it should determine the level of risks it is willing to accept and, given those risk tolerance rules, how far it is willing to deviate from these preestablished measures. Exhibit 6.7 outlines the relationship of these portions of the objective-setting component of COSO ERM. Starting with an overall mission, the approach is to (1) develop strategic objectives to support accomplishment of that mission, (2) establish a strategy to meet objectives, (3) define any related objectives, and (4) define risk appetites to complete that strategy. This exhibit was adapted from the COSO ERM guidance materials. These materials should be referred to for a more detailed understanding of COSO ERM. In order to manage and control risks at all levels, an enterprise needs to set its objectives and define its tolerances for engaging in risky practices and for its adherence to these rules. Things will not work if an enterprise establishes some risk-related objectives but then proceeds to ignore them.

(c) Event Identification

Events are enterprise incidents or occurrences—external or external—that affect the implementation of an ERM strategy and the achievement of its objectives. While our tendency is to think of events in a negative sense—determining what went wrong—they can be positive as well. Many enterprises today have strong performance-monitoring tools in place to monitor costs, budgets, quality assurance, compliance, and the like. However, going beyond just installing a meter on a production assembly line, monitoring processes should include:

- **External economic events.** A wide range of external events need to be monitored to help achieve an enterprise's ERM objectives. Both short- and long-term events can impact an enterprise's strategic objectives. As an external economic event example, in December 2001 and after some ongoing currency market turmoil, Argentina declared a major default of its public debt. This external event had a major impact on international credit markets, suppliers of agricultural commodities, and other business dealings in Argentina and throughout all of South America. External economic event identification here requires an enterprise to go beyond reported news headlines and raise the flag to suggest that such a currency default may highlight an enterprise risk-related event.
- **Natural environmental events.** Whether fire, flood, or earthquakes, numerous events can become incidents in ERM risk identification. Impacts here may include loss of access to some key raw material, damage to physical facilities, or unavailability of personnel.
- **Political events.** New laws and regulations as well as election results can have significant risk event-related impacts on enterprises. Many larger enterprises have a government affairs function that reviews developments here and lobbies for change, but such functions may not always be aligned with the enterprise's ERM objectives.
- **Social factors.** While an external event such as an earthquake is sudden and arrives with little warning, most social factors are slowly evolving events. These include demographic changes, social mores, and other events that may impact an enterprise and its customers over time. The growth of the Hispanic population in the United States is such an example. As more and more Hispanic people move to a city, for example, the teaching requirements in public schools and the mix of selections in grocery stores will all change.
- **Internal infrastructure events.** Enterprises often make benign changes that trigger other risk-related events. For example, a change in customer service arrangements can cause major complaints and a drop in customer satisfaction in a retail unit. Strong customer demand for a new product may cause changes in plant capacity requirements and the need for additional personnel.
- **Internal process–related events.** Similar to changes in infrastructure events, changes in key processes can trigger a wide range of risk identification events. In many cases, risk identification may not be immediate, and some time may pass before the process-related events signal the need for risk identification.
- **External and internal technological events.** Every enterprise faces a wide assortment of technological events that may trigger the need for formal risk identification. Some may be gradual while others, such as the shift to a Web environment, are more sudden. In other cases, a company may release a new

improvement that causes competitors everywhere to jump into action. Although the idea seems commonplace today, when Merrill Lynch, at the time a major brokerage, launched its Cash Management Account (CMA) concept in the mid-1980s, it caused a major stir in the financial services industries. CMA was a service that combined customer stock brokerage, bank checking accounts, and other financial services all under one roof. In the past, all such accounts were with separate providers with essentially no linkages between them.

An enterprise needs to define clearly its significant risk events and then have processes in place to monitor them in order to take any necessary appropriate actions. This forward-thinking type of process often is difficult to recognize in many enterprises. Looking at these internal and external potential risk events and deciding which ones require further attention can be a difficult process. Some are immediate needs, and others very future directed. The COSO ERM application techniques released material[5] offers some help here. The guidance material suggests enterprises consider some of these approaches:

- **Event inventories.** Management should develop risk-related listings of events common to the enterprise's specific industry and functional area. That is to say, an enterprise should consider establishing some type of a "lessons learned" archive source. Historically this is the type of data supplied by longer-tenure members of an enterprise who can offer "We tried this several years ago, but. . ." types of comments.
- **Facilitated workshops.** An enterprise can establish cross-functional workshops to discuss potential risk factors that may evolve from various internal or external events. The results from these workshops would be action plans to correct the potential risks. While the approach sounds good, it is often a challenge to allocate sufficient time to discuss such about risks format.
- **Interviews, questionnaires, and surveys.** Information regarding potential risk events can come from a wide variety of sources, such as customer satisfaction letters or employees exit interview comments. This information should be captured and classified to identify any that might point to a risk event.
- **Process flo analysis.** The COSO ERM application techniques materials recommend the use of flow diagrams to review processes and identify potential risk events. For many, these flow diagrams are similar to the internal control documentation prepared as part of SOx Section 404 documentation. That Section 404 work did not focus on risk event identification, but this ERM analysis can be combined with the Section 404 work in future update periods.
- **Leading events and escalation triggers.** The idea here is to establish a series of business unit measurements to monitor risk tolerance objectives and promote remedial action. For example, an enterprise's IT group may establish an objective to maintain strong security controls over the risk of a system intrusion. With a measure of the number of identified intrusion attempts during a period, a trigger of perhaps three intrusion incidents in a given month might trigger further action. Dashboard-type software tools or monitoring reports can be used here. These software tools are similar to the dashboard of an automobile, where indicators will flash signals for such conditions as low oil pressure or overheating. Risk status is reported through some simple, easy-to-comprehend graphic monitors, such as red, yellow, and green warning lights.

- **Loss event data tracking.** While the dashboard approach monitors risk events as they happen, it is often valuable to put things in more perspective after the passage of some time. Loss event tracking refers to using both internal and public database sources to track activity in areas of interest. These sources can also cover a wide variety of areas ranging from leading economic indicators to internal equipment failure rates. Again here, an enterprise should install effective risk identification processes to track both internal and external risk-related events.

The risk identification tools and approaches can yield some very useful information. Their use requires good analyses of the data as well as initiating plans for action, whether to shield from the risk or to take advantage of potential opportunities.

(d) Risk Assessment

While the internal environment component is COSO ERM's cornerstone (Section 4.3(h) discusses monitoring as its foundation), the risk assessment component is the framework's core. Risk assessment allows an enterprise to consider what effects potential risk-related events may have on an enterprise's achievement of its objectives. These risks should be assessed from two perspectives: the likelihood of the risk occurring and its potential impact. As a key part of this risk assessment process, however, is the need to consider inherent and residual risks as well:

- **Inherent risk.** As defined by the U.S. Government's Office of Management and Budget, inherent risk is the "potential for waste, loss, unauthorized use, or misappropriation due to the nature of an activity itself." Major factors that affect enterprise inherent risk are the size of its budget, the strength and sophistication of management, and just the very nature of its activities. Inherent risk is outside the control of management and usually stems from external factors. For example, the major retailer Wal-Mart is so large and dominant in its markets that it faces various inherent risks due to just its sheer size.
- **Residual risk.** This is the risk that remains after management responses to risk threats and countermeasures have been applied. There is virtually always some level of residual risk.

These two concepts imply that an enterprise will always face some risks. After management has addressed the risks that arose from the risk identification process, there still will be some residual risks to remedy. In addition, there always are some inherent risks that management can do little to mitigate. Wal-Mart, for example, can take some steps to reduce its inherent risks related to market dominance but can do essentially nothing regarding the inherent risk of a major natural earthquake.

Risk likelihood and impact are two other key components necessary for performing risk assessments. *Likelihood* is the probability or possibility that a risk will occur. In many instances, this can be a key management assessment stated in the terms of high, medium, or low likelihood of the risk occurring. There are also some good quantitative tools to develop likelihood estimates, but it does little good to estimate the likelihood of a risk occurring unless there is strong supporting data.

Estimating the *impact* if a risk event occurs is a bit easier. Examples include, for IT-related risks, the impact of a data server and network center catastrophic failure;

an enterprise can develop some relatively accurate estimates such as the cost of replacing facilities and equipment, the cost of restoring systems, and the cost of lost business due to the IT-related failure. However, the whole concept behind ERM is not to develop precise, actuarial-level calculations regarding these risks but to provide for an effective risk management framework. Detailed calculations can be delegated to insurance estimators and others.

An analysis of risk likelihoods and potential impacts can be developed through a series of quantitative and qualitative measures. Sources for more data are COSO ERM application techniques materials or the Project Management Institute's (PMI) special interest group on risk (www.risksig.com). These sources provide guidance on approaches to determine relative measures on risk likelihoods and potential impacts. The basic idea, however, is to assess all identified risks and to rank them in terms of likelihood and impact in a consistent manner.

Without going through a detailed quantitative analysis, each identified risk can be ranked on an overall relative scale of 1 to 10, with consideration given to the impact and likelihood of each. This ranking can be achieved by a focused management decision process where each of the identified risks is reviewed and then ranked with respect to this scale. Exhibit 6.8 shows how a series of risks for a sample

EXHIBIT 6.8 Risk Likelihood and Impact Mapping Example

Risk Name	Risk Definition	Impact	Likelihood	Risk Ranking
Accounting Risk	Failure to record sales activity accurately and timely may misstate financial reports.	High: Accounting errors may have a material impact on financial and operational information	Medium: Despite strong procedures, newer personnel in various location may make errors.	8
Legal Risk	Failure to understand current and changing laws and regulations may result in inability to comply with laws in multiple operations jurisdictions.	Medium: Even small, technical violations of most regulations should not have a material effect on operations.	High: With worldwide operations in multiple jurisdictions, violations—if only technical—can occur.	7
Segregation of Duties	Inadequately controlled segregation of duties may allow employees to process unauthorized, fraudulent transactions.	High: Fraudulent operations could have significant impacts on company operations.	Low: Ongoing internal audits and stronger management controls practices should prevent such control breakdowns.	5

company rated on a high, medium, or low relative values. For a larger enterprise, the risks could be scaled 1 to 10 to or even 1–100 allow greater granularity. The idea is to assign some relative rankings to risks and to identify those risks that should receive the most thorough management attention.

Overall approaches to reviewing these various likelihood and impact risks need to be considered. Risk assessment is a key component of the COSO ERM framework. This is where an enterprise evaluates all of the various risks that might impact its various objectives, considers the potential likelihood and impact of each of these risks, considers their interrelationship on a unit-by-unit or total enterprise basis, and then develops strategies for appropriate responses. In some respects, this COSO ERM risk assessment process is not too different from the classic risk assessment techniques that have been used for years. What is unique is that COSO ERM suggests that an enterprise should take a total approach, across all units and covering all major strategic concerns, to identify its risks in a consistent and thorough manner.

(e) Risk Response

Having assessed and identified its more significant risks, COSO ERM calls for measured responses to these various identified risks. There should be a careful review of estimated risk likelihoods and potential impacts, with consideration given to associated costs and benefits, to develop appropriate risk response strategies. These risk responses can be handled in any of these four basic ways:

1. **Avoidance.** This is a strategy of walking away from a risk—such as selling a business unit that gives rise to a risk, exiting from a risky geographic area, or dropping a product line. The difficulty is that enterprises often cannot drop a product line or walk away until after the risk event has occurred with its associated costs. Unless an enterprise has a very low appetite for risk, it is difficult to walk away from an otherwise successful business area or product line on the basis of a potential future risk. Avoidance can be a potentially costly strategy if investments were made to get into an area with a subsequent pullout to avoid the risk.

   A collective lessons-learned understanding of past activities often can help with this strategy. If the enterprise had been involved in some area in the past with unfavorable consequences, this may be a good way to avoid the risk once again. Due to constant changes and short employment tenures, this collective history is too often lost and forgotten. An enterprise's well-understood and communicated appetite for risk is perhaps the most important consideration when deciding if a risk avoidance strategy is appropriate.
2. **Reduction.** A wide range of business decisions may be able to reduce certain risks. Product line diversification may reduce the risk of too strong of a reliance on one key product line; splitting IT operations into two geographically separate locations will reduce the risk of some catastrophic failure. The number of effective strategies to reduce risks go down to the obvious and mundane, such as cross-training employees to reduce the risk of someone departing unexpectedly.
3. **Sharing.** Virtually all enterprises regularly share some of their risks through the purchase of insurance, but other risk-sharing techniques are available as well. For financial transactions, an enterprise can engage in hedging operations to protect from possible price fluctuations, or it can share potential business risks

and rewards through corporate joint venture agreements or other structural arrangements. The idea is to have another party accept some of a potential risk as well as to share in any resulting rewards.

4. **Acceptance.** This is the strategy of no action, such as when an enterprise self-insures by taking no action to reduce a potential risk. Essentially, an enterprise should look at a risk's likelihood and impact in light of its established risk tolerance and then decide whether to accept that risk or not. Acceptance is often an appropriate strategy for many of the various risks that an enterprise faces.

Management must develop a general response strategy for each of its risks using an approach built around one or a mixture of these risk avoidance strategies. In doing so, it should consider the costs versus benefits of each potential risk response as well as strategies that best align with the enterprise's overall risk appetite. For example, an enterprise's recognition that the impact of a given risk is relatively low would be balanced against a low risk tolerance that suggests that insurance should be purchased to provide a potential risk response. For many risks, appropriate responses are obvious and almost universally understood. An IT operation, for example, spends the time and resources to back up its key data files and implements a business continuity plan. There are typically no questions regarding the need for these basic approaches, but various levels of management may question the frequency of backup processes or how often the continuity plan needs to be tested. That is, they may question the extent and cost of planned risk prevention measures.

An enterprise should go back to its established risk objectives as well as the tolerance ranges for those objectives. Then it should readdress both the likelihoods and impacts associated with each to develop an overall set of the planned risk responses. This is perhaps the most difficult step in building an effective COSO ERM program. It is comparatively easy to identify a 5% likelihood risk that there could be a fire in the scrap materials bin and then to establish a risk response remedy to install a nearby fire extinguisher. However, responses to most risks are much more complex and require fairly detailed planning and analysis. If there is a risk that an enterprise could lose an entire manufacturing operation due to a key but old equipment plant production failure, potential risk responses might include:

- Acquire backup production equipment to serve as spare parts for cannibalization.
- Shut down the manufacturing production line with plans to move it elsewhere.
- Arrange for a specialized shop to rebuild/reconstruct the old equipment.
- Reengineer the manufactured product and plan for new product introduction.

Developing risk responses requires a significant amount of planning and strategic thinking. The several risk response alternatives may involve costs, time, and detailed project planning. For example, one of an older equipment response strategies is to acquire a set of backup equipment. If that is to be the approved strategy, action must be taken to acquire the backup equipment before this activity can even be identified as an actual risk response strategy. All risks listed on such an analysis should be measured against the same impact factors, based on an accept, avoid, share, or reduce risks strategy.

COSO ERM calls for risks to be considered and evaluated on an entity- or portfolio-wide basis. This can be a difficult process in a large, multi-unit, multi-product enterprise, but it provides a starting point in organizing these various risks to identify the more significant risks that may impact the enterprise. The idea here is to look at the potential risks, their probability of occurrence, and their impacts. A good analysis here should highlight areas for more detailed attention.

(f) Control Activities

ERM's control activities are the policies and procedures necessary to ensure action on identified risk responses. Although some of these activities may relate only to an identified and approved risk response in an area of the enterprise, they often overlap across multiple functions and units. The control activities component of COSO ERM should be tightly linked with the risk response strategies and actions previously discussed.

Having selected appropriate risk responses, an enterprise should select control activities necessary to ensure that the risk responses are executed in a timely and efficient manner. The process of determining if control activities are performing properly is very similar to completing SOx Section 404 internal control assessments (discussed in Chapter 4). COSO ERM calls for approaches of identifying, documenting, testing, and then validating these risk protection controls. After going through the COSO ERM risk event identification, assessment, and response processes, risk monitoring requires these four steps:

1. Develop a strong understanding of the significant risks and establish control procedures to monitor or correct for them.
2. Create fire drill–type testing procedures to determine if those risk-related control procedures are working effectively.
3. Perform tests of risk monitoring processes to determine whether they are working effectively and as expected.
4. Make adjustments or improvements as necessary to improve risk-monitoring processes.

This four-step process is similar to SOx Section 404 requirements to review, test, and then assert that internal control processes are working adequately. A major difference, of course, is that under SOx, an enterprise *is legally required* to assert the adequacy of internal controls. There are no such legal requirements at present with COSO ERM, but an enterprise should install risk-monitoring control activities to monitor the various risks it has identified. Because of the critical nature of many risks to an enterprise, risk monitoring can be very critical to an enterprise's overall health.

Many control activities under COSO internal controls are fairly easy to identify and test due to their accounting nature. These control activities generally include these internal control areas:

- **Separation of duties.** Essentially, the person who initiates a transaction should not be the same person who authorizes that transaction.
- **Audit trails.** Processes should be organized such that final results can be easily traced back to the transactions that created those results.

- **Security and integrity.** Control processes should have appropriate control procedures such that only authorized persons can review or modify them.
- **Documentation.** Processes should be appropriately documented.

These control procedures, and others, are fairly well recognized and applicable to all internal control processes in an enterprise and also may apply to many risk-related events. Many professionals, whether they have an accounting and auditing background or not, often can define some key controls necessary in most business processes. For example, if asked to identify the types of internal controls that should be built into an accounts payable system, many professionals would say that checks issued from the system must be authorized by independent persons, that accounting records must be in place to keep track of the checks issued, and that the check-issuing process should be such that only authorized persons can initiate such a financial transaction. These are generally well and widely understood internal control procedures. An enterprise often faces a more difficult task in identifying control activities to support its ERM framework. Although there is no accepted or standard set of ERM control activities at this time, the COSO ERM documentation suggests several areas:

- **Top-level reviews.** Senior managers should be very aware of the identified risk events within their organizational units and perform regular top-level reviews on the status of identified risks.
- **Direct functional or activity management.** In addition to top-level reviews, functional and direct unit managers should have a key role in risk control activity monitoring. This is particularly important where control activities take place within the separate operating units with the need for communications and risk resolution across enterprise channels.
- **Information processing.** Whether it is IT equipment-based processes or softer forms such as paper or messages, information processing represents a key component in an enterprise's risk-related control activities. Appropriate control procedures should be established with an emphasis on enterprise IT processes and risks.
- **Physical controls.** Many risk-related concerns involve physical assets, such as equipment, inventories, securities, and physical plants. Whether physical inventories, inspections, or plant security procedures, an enterprise should install appropriate risk-based physical control activity procedures.
- **Performance indicators.** The typical enterprise today employs a wide range of financial and operational reporting tools that also can support risk-event-related performance reporting. Where necessary, performance tools should be modified to support this important ERM control activity component.
- **Segregation of duties.** A classic control activity, the person who initiates certain actions should not be the same person who approves them.

These control activities are highlighted in the COSO ERM guidance materials. They can be expanded to cover other key areas. Some will be specific to individual units within the enterprise, but each of them, singly and collectively, should be important components of supporting the enterprise's ERM framework.

(g) Information and Communication

Although described as a separate component in the COSO ERM framework diagram in Exhibit 6.5, information and communication is less a separate set of risk-related processes than tools and processes linking other COSO ERM components. The concept is described in Exhibit 6.9 showing the information flows across the COSO ERM components. For example, the risk response component receives residual and inherent risk inputs from risk assessment as well as risk tolerance support from the objective-setting component. ERM risk response then provides risk response and

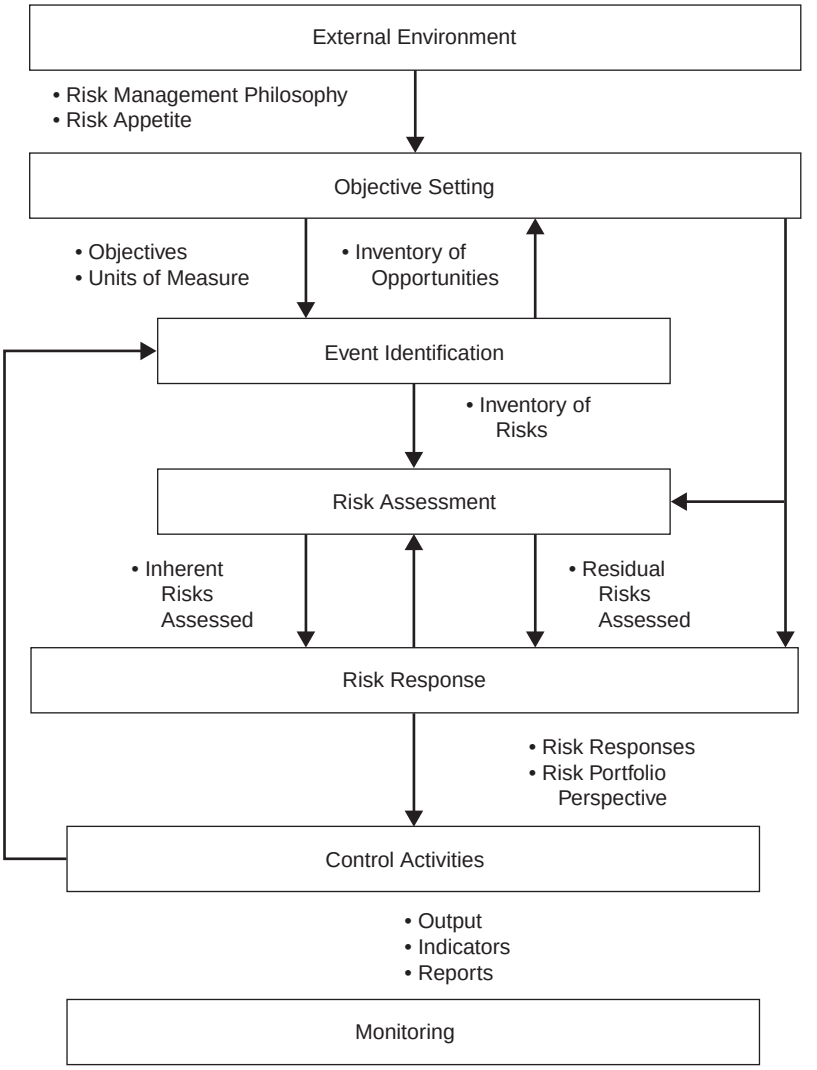


EXHIBIT 6.9 Information and Communication Flows in ERM Components

Source: COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework, Robert R. Moeller, Copyright © 2007 John Wiley & Sons. Reprinted with the permission of John Wiley & Sons, Inc.

risk portfolio data to control activities as well as feedback to the risk assessment. Standing alone, the monitoring component does not have any direct information connections but has overall responsibility for reviewing all of these functions.

While it is relatively easy to describe how information should be communicated from one COSO ERM component to another in a simple flow diagram, doing so is a far more complex process in practice. Basic processes in many enterprises consist of a complex web of operational and financial information systems that often are not very well linked. These linkages become even more complex for many ERM processes, given that many basic enterprise applications do not directly lend themselves to risk identification, assessment, and risk-response-type processes. Going beyond a comprehensive ERM information application for an enterprise, there is a need to develop risk monitoring and communications systems that link with customers, suppliers, and other stakeholders.

While the information segment of the ERM information and communication component is usually thought of in terms of IT strategic and operational information systems, the second aspect of this component, ERM communication, talks about communication beyond just IT applications. These include the need for mechanisms to ensure that all stakeholders receive messages regarding the enterprise's interest in managing its risks. There is a need for a common risk language throughout the enterprise regarding their risk management roles and responsibilities. COSO ERM will be of little value to an enterprise unless its importance is communicated to all stakeholders in a common and consistent manner.

(h) Monitoring

Placed at the base of the ERM framework model components, ERM monitoring is necessary to determine that all installed ERM components work effectively. People in the enterprise change, as do supporting processes and both internal and external conditions, but the monitoring component helps ensure that ERM is working effectively on a continuous basis. Examples of monitoring include processes to flag exceptions or violations in other components ERM processes. For example, an accounts receivable billing function should identify the overall financial and operational risks if customer bills are not paid on a timely basis. An ongoing—almost real time—credit collections monitoring tool could provide senior management with day-to-day and trending data on the status of collections. Dashboard monitoring tools, discussed previously, are ERM monitors that can work on a continuous basis.

Going beyond dashboard monitoring tools, enterprise management should take an overall responsibility for ERM monitoring. In order to establish an effective ERM framework, monitoring should include ongoing reviews of the overall ERM process ranging from identified objectives to the progress of ongoing ERM control activities. The COSO ERM Application Framework document suggests that monitoring could include these types of activities:

- Implementation of ongoing management reporting mechanisms such as for cash positions, unit sales, and key financial data. An enterprise should not have to wait until fiscal month-end for these types of status reports, and quick-response flash reports should be initiated.
- Periodic risk-related alert reporting processes should monitor key aspects of established risk criteria, including acceptable error rates or items held in

suspense. Such reporting should emphasize statistical trends and comparisons both with prior periods and with other industry sectors.
- Current and periodic status reporting of risk-related findings and recommendations from internal and external audit reports, including the status of ERM-related SOx identified gaps.
- Updated risk-related information from sources such as government-revised rules, industry trends, and general economic news. Again, this type of economic and operational reporting should be available for managers at all levels.

Separate or individual evaluation monitoring refers to detailed reviews of individual risk processes by a qualified reviewer, such as internal audit. Here the review can be limited to specific areas or cover the entire ERM process for an enterprise unit. Internal audit is often the best internal source to perform such specific ERM reviews. The role of internal audit in the ERM process and their role in monitoring, in particular, is discussed in next sections.

6.4 Other Dimensions of COSO ERM: Enterprise Risk Objectives

Although much of our COSO ERM introduction here is on the front-facing side of the three-dimensional framework, the two other dimensions—the operational and organizational levels—should always be considered. Each component of COSO ERM operates in this three-dimensional space; each must be considered in terms of the other related categories. The top-facing components of strategic, operations, reporting, and compliance risk objectives are important for understanding and implementing COSO ERM. In addition, while Exhibit 6.5 shows each of these top-facing risk objectives as having the same relative size, the operations-level risk objectives are often viewed as a much broader and higher-exposure risk category than the others.

(a) Operations Risk Management Objectives

Many types of operations risks can impact an enterprise. Following the three-dimensioned ERM framework, the operations-level risk objective calls for the identification of risks for each enterprise unit. This identification of operations-level risk objectives often requires detailed information gathering and analysis, particularly for a larger enterprise covering multiple geographic areas, product lines, or business processes. Direct managers of individual units usually have the best understanding of their operational risks, and that information can become lost when consolidated for higher-level reporting. Internal audit reviews or surveys of persons directly impacted by these risks can help to gather more detailed background information on potential operations risks. A survey of direct on-the-floor members of the enterprise, along with follow-up questions, will allow the development of a broad and consistent set of cataloged operations risks. The questions asked here would be similar to the types of detailed questions used in internal audit internal control assessments, and the results here could become a basis for developing a better understanding of the potential risks.

These types of surveys, circulated at all levels of an enterprise, with a message encouraging stakeholders to respond candidly, often gather important information regarding potential risks at a detailed operational level. A manager of a remote

operating plant may not have adequately communicated concerns about some plant-level operational risk. Often a broadly based and confidential survey better allows people to communicate local-level operations risks up through the enterprise.

With ERM's portfolio view of risks, an enterprise should avoid rolling things up into too much of a summary level, missing or rounding off important lower-level risks. Whatever their position in the enterprise or their geographic location, managers at all levels should be aware that they are responsible for accepting and managing the risks within their own operational units. Too often, unit managers may believe that risk management is of concern only to senior-level headquarters staff. The importance of COSO ERM and operations risk management should be communicated to all levels of an enterprise. Internal auditors should act as eyes and ears here and report all observed operations risks.

(b) Reporting Risk Management Objectives

This risk objective covers the reliability of an enterprise's reports of internal and external financial and nonfinancial data. Accurate reporting is critical to an enterprise's success in many dimensions. News reports often detail the discovery of inaccurate corporate financial reporting and resulting stock market repercussions for the offending entity. That same inaccurate reporting can cause problems in many areas. An example of the risks related to inaccurate reporting became an issue several years ago at the major petroleum company Royal Dutch Shell. Oil and gas exploration companies are required to report on their reserves—the amount of oil and gas on their properties that have not yet been extracted. In January 2004, Royal Dutch announced that due to bad estimates and sloppy record keeping, it had been significantly overreporting estimated petroleum reserves.[6] This error did not affect the company's reported financial results and SEC reserve reporting guidelines here are not that strong; nevertheless, the market battered the stock after the announcement, and the CEO, the head of oil exploration operations, and others were forced to resign. The company, under a new chairman, then announced a raft of changes and internal control improvements to repair the damage.

No matter what industry it is in, an enterprise faces major risks from inaccurate reporting at any unit or area. Operating units must make certain that reported results are correct before they are passed up to the next level in the organization, and consolidated numbers must be accurate, whether they are on financial reports, tax returns, or any of a myriad of other areas. Good internal controls are necessary to ensure accurate reporting. ERM is concerned about the risk of authorizing and releasing inaccurate reports. Strong internal controls should minimize the risk of errors, and an enterprise should always consider the risks associated with inaccurate reporting. Royal Dutch Shell reserve reporting errors are an example of this type of risk reporting concern. Small errors and discrepancies can be ignored over time until there is a major error that needs to be disclosed. The risk of such inaccurate reporting should be a concern at all levels of the enterprise.

(c) Legal and Regulatory Compliance Risk Objectives

Any type of enterprise must comply with a wide range of laws and government-imposed or industry standards regulations. While compliance risks can be monitored and recognized, legal risks are sometimes totally unanticipated. In the United States,

for example, an aggressive plaintiff legal system can pose a major risk to otherwise well-intentioned enterprises. Asbestos litigation during the 1990s and beyond is an example. Asbestos, a fibrous mineral, has three extraordinary characteristics: It works as an insulator for heat and electricity; it resists other dangerous chemicals; and, when inhaled, it has now been found to cause illnesses that can take decades to develop. A natural insulation material, asbestos was used extensively in building materials and considered benign. Too much direct contact with asbestos fibers over time, however, can cause severe lung problems and even death. Underground miners extracting asbestos have met that fate. However, in the past, asbestos was used in many products, such as wrappers to insulate heating pipes or as fire protection wall barriers. The risks to persons working or living in a structure with asbestos-sealed pipes are fairly minimal, but aggressive litigators have brought actions against corporations, claiming that anyone who could have had *any* contact with a product that used asbestos could be at risk sometime in the future. The result was litigation directed against companies that had manufactured products containing some asbestos, calling for damages based on potential human risks in future years. Because of huge damage awards, virtually all major corporations that once used asbestos have gone bankrupt, are out of business, or have had to pay huge court-imposed damage losses. This type of legal risk is very difficult to anticipate but can be disastrous to an enterprise.

COSO ERM recommends that compliance-related risks be considered for each of the risk framework components, whether in the context of the internal environment, objective setting, or risk monitoring, as well as across the enterprise. The ERM guidance material does not offer much additional information on this compliance objective other than to state that this objective refers to conformance with applicable laws and regulations. These are important elements of the risk management framework that need to be communicated and understood.

As has been discussed, all enterprises face a wide range of legal and regulatory compliance requirements, with some impacting virtually all enterprises and others related to only single business units in a specialized industry sector. The nature of those compliance risks needs to be communicated and understood through all levels of an enterprise. An enterprise may accept a certain level of risk in terms of its concerns regarding legal compliance. While a major law should never be deliberately ignored because of a feeling the transgression never will be caught, an enterprise should always take a reasoned approach to risks in conjunction with its overall philosophy and risk appetites. For example, many regulatory rules specify that all expenditures must be supported by a receipt. While there usually are no specific reasonableness guidelines, one enterprise could decide that "all expenditures" goes down to an employee travel expenses of less than $1, while another will require receipts of anything above $25. The latter enterprise has made a decision that the costs of documenting these small expenditures is greater than any fine it might receive if caught in a regulatory compliance issue. This type of a risk-related decision is similar to the new AS 5 financial internal controls rules for SOx discussed in Chapter 4. In order to manage and establish legal and regulatory risk objectives, the board of directors, CEO, and members of management need to understand the nature and extent of all regulatory risks that the enterprise faces. The legal department, key managers, internal audit, and others can help in assembling this information. There are many regulatory enterprise-level risks ranging from major to minor, but regulatory risks are never "minor" when an enterprise is found to be in legal violation of one or another of them.

6.5 Entity-Level Risks

The third dimension of the COSO ERM framework calls for risks to be considered on an organization or entity-unit level. The COSO ERM framework in Exhibit 6.5 shows four divisions in this framework dimension: entity level, division, business unit, and subsidiary risks. This is not a prescribed company-type division, and ERM suggests that risks should closely follow the official organizational chart. COSO ERM risks should be identified and managed within each significant organizational unit, including risks on an entity-wide basis through individual business units.

An enterprise with four major operating divisions and with multiple business units under each would have an ERM framework that reflects all of these units. While these risks may be important to the overall organization, they should be considered on a unit-by-unit basis to as low a level as necessary to allow the enterprise to understand and manage its risks. COSO ERM does not specify how thinly these unit-level risks should be sliced, and the criticality and materiality of individual business units should be considered. For a major fast-food restaurant chain with thousands of units, for example, it would not be reasonable to include each individual unit as a separate component in the risk model. Rather, management should define its organizational-level risks in enough detail to cover all significant, manageable risks.

(a) Risks Encompassing the Entire Organization

Multiple risks at the business unit level should roll up to entity-level risks. It is easy for an enterprise to consider some unit-level risks as being "not material"; to use pre-SOx public accounting terminology, an enterprise has to think of all risks as potentially significant. For example, consider a relatively small subsidiary in a developing country that is manufacturing casual clothing. Often such a unit is so small in terms of total corporate revenue contributions or its relative size that it can slip under the radar on a senior corporate level. However, if there were child labor issues in the host country, the enterprise may find itself at the center of attention regarding this small subsidiary operation. In such a situation, journalists may ask the CEO to publicly comment on policies and procedures at that subsidiary operation, even though the CEO may know of its existence only vaguely.

Our point here is that both major as well as seemingly small risks can impact an entire enterprise. The delivery of tainted food produced at one small unit of a large fast-food chain can impact the prospects and reputation of the total enterprise. It is relatively easy to identify high-level entity-wide risks, such as compliance with SOx Section 404, and to identify and monitor these as part of the COSO ERM process, care must be taken that smaller potential risks do not slip through the cracks. As risks are identified through organization-wide objective setting, they should be considered on an entity-wide basis as well as by individual operating units. Those individual unit risks should be reviewed and consolidated first to identify any key risks that may impact the overall organization. In addition, any organization-wide risks should also be identified.

(b) Business Unit–Level Risks

Risks occur at all levels of an enterprise, whether a major production division with multiple plants and thousands of employees or a minority ownership position in

a foreign country sales company. Risks must be considered in each significant organizational unit. Even the risks identified in the minority ownership position in a foreign country sales company, for example, may be risks unique to that unit but then should roll up to the overall entity. We have cited the example of entity-level risks that might result from failures in manufacturing or human rights standards from a small subsidiary in a developing country. Risk events here can cause an embarrassment to the overall enterprise, but they should have been controlled all the way down to that small-company unit. The Bhopal, India, plant explosion disaster brought down the parent corporation, as mentioned.

Depending on the complexity and number of operating units, risk responsibility often can best start as a push-down process where corporate-level management formally outlines major risk-related concerns and asks responsible management at each of the major divisions to survey risk objectives through the operating units within that division. In this manner, significant risks can be identified at all levels and then managed at levels where they can receive the most direct, local support.

A major concept surrounding COSO ERM is that an enterprise faces a wide range of risks at all levels. Some may be significant while others are often just troubling annoyances and viewed as minor. The COSO ERM framework provides a mechanism to consider these risks; it is an important tool to help ensure SOx compliance.

6.6 Putting It All Together

The COSO ERM framework described here addresses a risk management approach applicable to all industries and encompassing all types of risk. With its focus on recognizing an enterprise's appetite for risk and the need to apply risk management within the context of overall strategy setting, the COSO ERM has some fundamental differences from most risk models that have been used to date. COSO ERM has not been in use long enough to point to a series of successful enterprises that have publicly embraced it. However, with the AS 5 emphasis on risk, we will be hearing more about it going forward. Internal auditors, in particular, should establish a CBOK objective to learn more about this important framework.

COSO ERM arrived after SOx, but is an important tool for managing and understanding SOx Section 404 internal controls. It is particularly important with the newer AS 5 auditing standards that give more consideration to risk when understanding and evaluating internal controls. Enterprise management at all levels should embrace COSO ERM, an important tool for understanding the many the multiple risks an enterprise faces today. Internal auditors should make COSO ERM an internal audit CBOK requirement, and should perform internal audits of compliance with ERM processes.

6.7 Auditing Risk and COSO ERM Processes

Internal auditors will encounter risk and risk management issues in many areas of the audit universe where there are performing reviews, and effective internal auditors should understand risk management processes. All too often, an internal auditor will be performing an internal controls review in some area and will be told that the area was or was not selected because of "risk considerations." The auditor should have

a CBOK level of knowledge of basic risk management processes to be able to ask the right questions and to review the adequacy of those processes.

An enterprise can improve its overall processes as well as SOx internal controls processes through an effective and efficient implementation of COSO ERM. By focusing on the COSO ERM framework as well as general good risk management practices, internal audit can help an enterprise by planning and performing reviews of enterprise risk-management processes. Of course, to review COSO ERM practices and implementation procedures, internal auditors, either as internal audit reviewers of controls or consultants to management, need to develop a strong understanding of COSO ERM controls and processes. In addition, any internal audit review of enterprise ERM processes should be developed through the risk-based internal audit planning approaches discussed in Chapter 15. Internal audit should review enterprise-wide ERM processes using some of these tools:

- **Process flowcharting** As part of any identified ERM process, process flowcharts can be useful in describing how risk management operates in an enterprise. This requires looking at documentation prepared for risk-related processes, determining if they are current conditions, and describing the overall adequacy of all levels of enterprise risk processes. Internal audit process modeling and process flowcharts are discussed in Chapter 16.
- **Reviews of risk and control materials.** An ERM process often results in a large volume of guidance materials, documented procedures, report formats, and the like. There may often be valuable to an internal audit review the risk and control materials.
- **Benchmarking.** Although an often misused term, *benchmarking* is the process of looking at functions in another environment to assess their operations and to develop improved approaches based on the best practices of others. The Institute of Internal Auditors' (IIA's) "Progress Through Sharing" motto and tradition as well as benchmarking approaches discussed in Chapter 11 promote the gathering comparative information. This often can be a useful technique here.
- **Questionnaires.** Questionnaires are a good method for gathering information on ERM effectiveness from a wide range of people. They can be sent out to designated stakeholders with requests for specific information. This is often a valuable internal audit technique.

Internal audit should establish some high-level review objectives for the effectiveness of COSO ERM in their enterprise, gather detailed implementation data, and then assess the effectiveness of COSO ERM and as a tool to support and enhance SOx compliance. Exhibit 6.10 provides guidance for auditing COSO ERM Internal Audit Procedures.

6.8 Risk Management and COSO ERM in Perspective

Because the two framework models look quite similar on first observation, it is very easy to overlook the unique characteristics of COSO ERM. It took many years for COSO internal controls to be recognized as more than an interesting technical study. It had been first codified as an auditing standard by the American Institute of

EXHIBIT 6.10 Auditing COSO ERM Internal Audit Procedures

Step	Audit Procedure	Initial	W/P
1	Meet with appropriate managers to gain an understanding of the enterprise's ERM implementation strategy, its planned scope, and current implementation status.		
2	Develop a strategy for reviewing ERM processes, perhaps with a focus emphasizing all internal environment processes on an entity level as well as the status of all components for a selected subsidiary or business unit.		
3	Develop detailed internal audit plans for the components selected for reviews and publish engagement letters announcing the planned audits.		
4	Review enterprise-wide ERM guidance materials in place to assess whether ERM objectives are being adequately communicated, and assess areas where communication may be lacking.		
5	Risk management philosophy and appetite.		
5.1	Meet with appropriate members of management to assess whether a risk management philosophy has been defined and communicated.		
5.2	Through surveys or interviews, meet with selected members of the enterprise to determine if the risk appetite has been communicated.		
6	Risk management integrity and ethical values.		
6.1	Review published codes of conduct and other materials to determine if risk-related ethical values are being communicated.		
6.2	Review a sample of enterprise communications and assess whether attention is given to ERM philosophies.		
7	Risk management organization structure.		
7.1	Meet with human resources management to assess whether processes are in place to communicate ERM philosophy to enterprise.		
7.2	Review code of conduct records to determine that it has been periodically updated, that all stakeholders have acknowledged it, and that code compliance records are in place.		
7.3	Based on a review of organization charts and other documentation, assess whether ERM philosophy appears to be in place throughout selected units in the enterprise.		
8	Select one subsidiary or enterprise unit to determine if enterprise-wide ERM objectives and risk components are in place for the selected unit.		
8.1	Assess compliance with ERM internal objectives for the selected business unit.		
8.2	Assess compliance with ERM objectives setting processes for the selected business unit.		
8.3	Assess compliance with ERM event notification processes for the selected business unit.		
8.4	Assess compliance with ERM risk assessment for the selected business unit.		
8.5	Assess compliance with ERM risk response processes for the selected business unit.		
8.6	Assess compliance with ERM control activity processes for the selected business unit.		
8.7	Assess compliance with ERM information and communication processes for the selected business unit.		
8.8	Assess compliance with ERM risk monitoring processes for the selected business unit.		

Certified Public Accountants' Auditing Standards Board (ASB) and received some mention in IIA publications, but it took SOx to give COSO internal controls some serious recognition. The initial SOx legislation talked about an internal accounting standard "to be established." Later the Public Company Accounting Oversight Board (PCAOB) mandated that COSO internal controls should be the internal control review standard. Arriving after SOx, COSO ERM does not yet have that same level of recognition. The IIA was an important early proponent, and elements of ERM can be seen in its new version of the *C*ontrol *ob*jectives for *i*nformation and related *T*echnology (CobiT) framework (see Chapter 5), but it still is not at the same level of importance and significance today for an enterprise as COSO internal controls.

This recognition may take some time. As mentioned, there has been some confusion because the two frameworks look alike and have *COSO* in their names. However, the risk-related emphasis of the new AS 5 auditing standards as well as an increasing recognition of risk issues in professional literature has increased professional interest in and attention toward enterprise risk management, particularly when attempting to achieve SOx internal control compliance. The three-dimensional ERM framework helps to place risk and internal control issues in a better perspective when evaluating SOx compliance.

Risk management and COSO ERM, in particular, are knowledge skills that should be part of every internal auditor's CBOK. Internal auditors should use risk management principles when deciding which areas to select for their reviews (as discussed in Chapter 15) and then use risk principles when assessing audit evidence (as discussed in Chapter 9). Perhaps even more important, COSO ERM will grow in importance and recognition as more enterprises understand and adopt the ERM framework. Internal audit should have a CBOK understanding of COSO ERM both in order to audit compliance to these processes and to consult with management to ensure more effective implementations.

Notes

1. "Bhopal 'Faces Risk of Poisoning,'" November 14, 2004, http://news.bbc.co.uk/2/hi/south_asia/4010511.stm. Note: This is one of Web many references on this issue. A search for "Bhopal, India" and "Dow Chemical" will yield a large amount of information.
2. "COSO Releases a New Risk Management Framework," *Accounting Today,* October 25, 2004.
3. Committee of Sponsoring Organizations, *Executive Risk Management—Integrated Framework: Executive Summary Framework,* September 2004, www.coso.org
4. Six sigma is a disciplined, methodology for eliminating defects (driving toward six standard deviations between the mean and the nearest specification limit) in any process, from manufacturing to transactional and from product to service.
5. COSO, *Executive Risk Management—Integrated Framework.*
6. "Reporting Problems at Shell," *The Guardian* (London), www.ruesges.com, March 24, 2004.

PART III

Planning and Performing Internal Audits

CHAPTER 7

Performing Effective Internal Audits

The book covers many modern internal auditing common body of knowledge (CBOK) requirements, including basic internal control standards, communicating with the board of directors audit committee, and performing specialized internal audits in such areas as information technology (IT) security controls. This chapter goes through the basic steps and processes necessary to plan, perform, and complete an individual internal audit. While many additional steps for building an internal audit function are covered in other chapters, we start this chapter with the assumption that an effective enterprise internal audit function exists with an approved audit charter as well as with audit committee approval for an annual plan of its internal audit activities. This chapter goes through the steps necessary to perform an internal audit review of internal controls. Virtually all internal audits start with the establishment of an approved internal audit charter, a reaffirmation of initial audit objectives, the development of a detailed individual audit plan, and then a program of actual internal audits including the initial review and documentation of internal controls, tests to determine they are working as expected, and subsequent reports on the results of the audit. This chapter describes one of internal audit's core CBOK requirements.

An effective internal auditor serves as a front-line set of eyes and ears for the audit committee and senior management, and must do more than just review the enterprise's compliance with published documentation and procedures. Internal auditors visit facilities where the enterprise's actual work is performed and records are maintained, observing operations and providing management-level reports. Internal auditors can then observe and develop an understanding of processes in place and design and perform appropriate tests to evaluate supporting internal controls. This chapter introduces procedures to organize, plan, and perform these internal audits, including surveys, assessments of internal controls, workpaper documentation, and administrative controls for managing internal audits. These procedures are appropriate for virtually all operations, whether an audit of a remote operational area covering manufacturing resource planning or a corporate headquarters financial area such as an accounts payable function. These same procedures are also appropriate for specialized audits, such as reviews of telecommunications or IT controls. The basic steps to perform internal audits discussed in this chapter are useful for performing most internal audits.

Our example audit is based on a review of a hypothetical sample company, Global Computer Products, a manufacturer and distributor of IT security hardware and software with operations in the United States, India, and the Netherlands.

(Chapters 7 through 11 on planning and performing internal audits as well as Chapters 12 through 17 on organizing and managing internal audit activities also refer to this same hypothetical company.)

7.1 Organizing and Planning Internal Audits

The overall steps and processes for organizing and planning internal audits require a general understanding the Institute of Internal Auditors' (IIA's) *International Standards for the Professional Practice of Internal Auditing* discussed in Chapter 8, as well as knowledge of supporting internal audit guidance tools described in Chapters 9, 10, and 11. For example, although this chapter walks us through the steps necessary to conduct an internal audit, Chapter 17 explains how to prepare workpapers and communicate results through audit reports. Of course, the overall internal audit process requires a well-organized and managed internal audit function, as outlined in Chapters 12 through 17. Internal auditing requires a wide range of interrelated skill and knowledge areas that cannot be described as one sequential set of action steps but include many interrelated activities.

This chapter outlines general steps for performing an internal audit, focusing on an internal controls review of the purchasing and accounts payable processes at our example company, Global Computer Products. Our company must purchase parts to add to its production cycle and pay for those goods through supporting accounting processes.

However, before an internal audit function can launch any audits, it needs some building blocks in place to establish an effective internal audit function. As explained in other chapters, these internal audit foundation building blocks include:

- **An effective plan of organization and a charter for launching internal audit activities.** Chapter 12 suggests procedures for building an effective internal audit function, and Chapter 23 describes sample charters to authorize an internal audit function.
- **A long-range or annual audit plan.** Any individual internal audit should be based on a longer-range plan of audit activities. Chapter 15 discusses risk-based audit planning and, of course, emphasizes that long-range audit plan would have been approved by the audit committee. This chapter starts with the development of the long-range audit plans to begin the actual internal audit.
- **Standard and effective approaches for performing all internal audits.** Chapter 8 discusses the IIA's *International Standards for the Professional Practice of Internal Auditing,* fundamental requirements for all internal audits, and Chapter 13 outlines a series of key competencies necessary to perform these internal audits.

Of course, these are not the only key CBOK tools necessary to perform effective internal audits. Among other matters, internal auditors need to develop good approaches for evaluating audit evidence (see Chapter 9), effective audit results reporting (see Chapter 17), a strong understanding of the Committee of Sponsoring Organizations' (COSO) internal controls framework (see Chapter 3), and a consistent framework for evaluating those controls (see Chapter 5).

Starting with steps for planning an internal audit and then continuing through a variety of audit processes, this chapter outlines the steps necessary for an internal controls review of the production parts purchasing cycle at a unit of our sample company, a representative internal audit. Our objective here, and in other supporting chapters, is to suggest a series of internal audit procedures for performing reviews. Whether as an individual professional or as the enterprise's internal audit function, internal audit is more effective if all members of the audit staff follow consistent, professional procedures in performing their reviews. They will become a strong enterprise resource in the eyes of management, who should expect consistent, quality approaches from the internal audit resources.

7.2 Internal Audit Preparatory Activities

Each internal audit project should be carefully planned prior to its start. Audits should be initiated as a scheduled element in internal audit's annual planning and risk-assessment process, as discussed in Chapter 15, through a management or audit committee special request, or in response to unplanned events, such as the discovery of a fraud, new regulations, or unexpected economic events. Some internal audits will be updates or repeats of reviews performed in prior periods, such as an update of some internal controls and testing as part of a review of a Sarbanes-Oxley (Sox) Section 404 key process, but internal audit has a need to launch new internal audit reviews regularly. Whether a planned periodic review of some area of operations or a new audit requirement that was identified because of some unexpected event, internal audit needs to develop a plan for any new audit.

Exhibit 7.1 shows a high-level "memo to files" document describing an upcoming planned audit. This is the type of document an internal audit manager might prepare to outline an upcoming planned audit at a very high level. This type of documentation is designed primarily for the internal audit team. However, since the audit is still in its very preliminary stages here, such a document usually is not shared with auditees at this point. Such a preliminarily planned audit would then be built into an annual audit plan. Using our Global Computer Products example enterprise, internal audit would build such an annual plan to outline its planned activities over a future period. This type of plan would be approved by the audit committee and would be updated periodically as internal audit reports progress to the audit committee. Exhibit 7.2 shows an example of a short-term schedule (three months) for upcoming planned internal audits. In this chapter, we outline the steps necessary for a new internal audit covering purchasing and accounts payable internal controls at Global Computer Products. The audit was initially scheduled based on some high-level stated objectives and hour estimates, and the process brings us from such a high-level annual internal audit plan to steps for getting ready to perform the actual internal audit.

After internal audit has developed a plan for work over the coming year, planning and scheduling individual internal audits often can be a challenge. Despite well-thought-out plans, unscheduled events, requests from management, or situations such as unfavorable results from other audits may cause changes in an internal audit long-range plan. While there often are pressures to begin such special audits immediately, a properly planned audit will almost always provide better audit results. In addition, internal audit can obtain significant savings in time and effort with adequate advance planning and preparatory work.

EXHIBIT 7.1 Audit Planning Memo Sample

Global Computer Products

February 2, 20xx

To: Workpaper Files
From: L. C. Tuttle, Audit Supervisor
Subject: Accounts Payable Systems Audit Planning Memo

This memo is to document the planned review of key purchasing and accounts payable processes at Global Computer Products manufacturing facility at Minneapolis, MN. The review will be performed by two members of our internal audit staff with L. C. Tuttle as project leader and Herman Hollerith providing support for our review of network and IT systems controls.

The objective of this review will be to assess the adequacy of purchasing system internal accounting controls at the Global Computer Products Minneapolis facility as well as the purchasing processes at multiple branch facilities, interfaces to the accounts payable system at corporate headquarters, and automated systems to support these processes.

The audit is scheduled to begin on about March 15, 20xx and has been budgeted for a total of XX hours of time from the on-site audit team. A detailed plan, including expect hours by each auditor, will be prepared prior to the start of this review.

The review will emphasize controls over linkages from the purchasing system to other enterprise manufacturing database systems. In addition, the review will update documentation and perform tests, as necessary, to support SOx Section 404 requirements covering this process. All recommendations and audit findings will be reported in a normal internal audit department report.

L. C. Tuttle, Audit Supervisor
W. J. Rawdon, Audit Manager

EXHIBIT 7.2 Audit Plan Project Schedule Example

GLOBAL COMPUTER PRODUCTS INTERNAL AUDIT DEPARTMENT
FEBRUARY, MARCH, AND APRIL AUDIT PROJECT SCHEDULE

PROJECT #	AUDIT	AUDITOR	ACTIVITY	FEB	MAR	APR
A23-06	A/P - Purchasing Minneapolis Review	Hollerith	Test IT Controls	20	80	45
A23-06	A/P - Purchasing Minneapolis Review	Spatz	Document Processes	110	24	12
A23-06	A/P - Purchasing Minneapolis Review	Prusch	Tests of Transactions	36	80	12
A23-06	A/P - Purchasing Minneapolis Review	Tuttle	Manage Audit	12	18	20
A28-78	Branch Sales Offices	Bushman	US West Regions	120	145	30
A28-78	Branch Sales Offices	Lester	US West Regions	0	68	160
A31-01	Job Control Review	Doe	Document Processes	0	64	80
A31-01	Job Control Review	Hollerith	Test IT Controls	0	40	40
A31-01	Job Control Review	Tuttle	Manage Audit	8	12	12

Although a small element of the preparatory activities described in this chapter can be performed concurrent with the audit itself, most normally must take place in advance of visiting the audit site or beginning the actual internal audit. These important preparatory activities include defining the objectives, scope, and procedures of the audit program to be used in an individual audit. This is particularly important in larger organizations performing multiple, concurrent audits with different mixes of audit personnel assigned to each.

While no single internal audit is really typical and most have unique characteristics, general internal audit planning activities outlined here normally are done well in advance for most internal audits. Relative risks (see Chapter 15) should have been considered as part of the long-range audit plan leading up to each individual internal audit. Once the need for the new audit has been identified, the next steps are to define or reaffirm the specific audit objectives, work out logistics arrangements for the review, and then develop a detailed individual audit plan for that review.

(a) Determine the Audit Objectives

Internal audit should generally establish plans for internal audit activities that typically cover a fiscal year period. These long-range plans are based on management and audit committee requests, audit staff capabilities, the nature of prior audit work, available resources, and general risks facing the enterprise. This long-range, risk-based internal audit planning process (discussed in Chapter 15) paints a big-picture activity list for internal audit. However, changes in business operations and the general economy, problems identified through other internal audits, new laws and regulations, audit staff changes, or any of a variety of other issues may somewhat alter that long-range audit plan over time. These overall audit plans should include high-level objectives for each planned audit as well as an understanding of the surrounding risk environments.

A high-level objective statement should be established for each individual planned audit. These audit objective statements do not have to be detailed lists of requirements but should have sufficient information to tell the auditee, management, and others what internal audit is trying to accomplish when launching an internal audit in some area. Here are some examples of internal audit objective statements:

- . . . to assess the adequacy of purchasing system internal accounting controls at the Global Computer Products Minneapolis facility as well as the purchasing processes at multiple branch facilities, interfaces to the accounts payable system at corporate headquarters, and automated systems to support these processes.
- . . . to update documented processes and test internal controls, as necessary, for fixed asset management processes to satisfy their SOx Section 404 requirements.
- . . . to review the internal controls in place over maintenance for the IT configuration management database and its supporting procedures.

Each of these brief statements describes what internal audit is planning to accomplish in an upcoming review. While the project can be expanded as the reviews get started, these objective statements get an internal audit started. Over the course of an approved, planned audit, the objective statement should always be viewed as the big picture describing internal audit objectives for a given review.

Although closely related to the planned objective statement, it is sometimes valuable to add a scope statement as well. For example, an audit scope statement can identify a planned review of quality management production processes in international operations; a scope statement might, for example, limit the review to only Australia/New Zealand operations. The scope statement words better define what the new audit is trying to accomplish.

These internal audit preliminary objective and scope statements should be reviewed with management or others requesting the audit. An effective way to describe these internal audit plans is through an audit planning memo. This communication, although it is not presented directly to the auditee yet, describes what internal audit is planning to accomplish, who will be doing the review, and its approximate timing. Such a memo is an essential starting document for the workpapers, as described in Chapter 16, to begin documenting that internal audit. Exhibit 7.1 shows a sample audit planning memo where an internal audit supervisor outlines the objectives of a planned internal audit, who will be assigned to do the work, and its estimated timing. Of course, even though our exhibit shows a memo from the old hard-copy paper days, a planning memo today would almost certainly be an electronic document.

(b) Audit Scheduling and Time Estimates

The approved annual internal audit plan, discussed in Chapter 15, outlines which internal audits are to be performed in any given period. Key internal audit staff members and managers should have participated in this planning process and be aware of ongoing needs for any subsequent plan adjustments. Preliminary time estimates are established and time frames set for performing each audit. However, changes often are made to this annual plan during the course of the year due to the increased resource requirements of other audits in progress, revised audit scopes, personnel changes, and other management priorities.

In addition to the annual plan and its revisions, individual audit schedules should be prepared based on this plan. Depending on the nature of the audits performed and audit staff size, these individual schedules may cover a month, a quarter, or even a longer period. For a larger internal audit group, detailed audit schedules should be prepared for both the entire audit department as well as individual auditors and reviewed at least monthly to reflect changes or adjustments. For example, an internal audit specialist in a key area may be unavailable for several weeks or months. This might require an overall shift in audit department plans.

The number and level of staff required for various audits depends on an evaluation of the nature and complexity of the audit projects as well as auditor abilities and time constraints. Audit projects should be broken down into individual tasks for making these audit project hour estimates. Overall estimates then are more reliable and can serve as a benchmark for comparing actual with budgeted audit performance. Of course, the plans developed at an early stage of the audit often are preliminary and must be adjusted once more information is obtained.

Auditor skills and developmental needs should be considered in selecting personnel for any audit project assignment. After deciding on the individual audit segments, the talents needed to perform the audit tasks must be determined. For example, one segment of a planned audit may require an information systems audit specialist to evaluate certain IT controls while another segment may require an auditor with audit-sampling skills to construct and evaluate a statistical test.

(c) Preliminary Surveys

The annual risk-based long-range audit plans discussed in Chapter 15 as well as the high-level planning memo shown in Exhibit 7.1 should have been made with knowledge of the expected areas to be audited. For example, audit management would realize that a branch office review should take *about* X hours to complete based on past experience; however, risk analysis for annual audit planning often should be performed at a high or overview level. There is often a need to go beyond those annual-plan-hours estimates before starting the actual audit. If plans are for a review of an area previously reviewed, a good first step should be a preliminary survey that gathers background materials regarding the entity to be audited. This survey is often the responsibility of audit management or the designated in-charge auditor. These items should be reviewed, if available, during an internal audit preliminary survey:

- **Review of prior workpapers.** The prior audit objectives and scope, audit workpapers, and programs used should be reviewed to gain familiarity with approaches used and the results of those audits. Internal audit self-assessment critiques, prepared at the end of each review and discussed in Chapter 11, help to better understand the prior review approaches used and the alternatives available. Special attention should be given to any problems encountered in the prior audit and the suggested methods of solving them. The organization of internal audit workpapers is discussed in Chapter 16.

  Knowing the amount of time the prior audit took as well as any problems encountered can help determine resources needed for the planned audit. The results of prior tests performed should be reviewed, with decisions made on whether any should be reduced, eliminated, expanded, or performed on a rotating basis in future audits. Prior workpapers may indicate that a large sample of test-count items was included as part of an inventory review, but due to generally good internal control procedures, few problems were encountered. Planning for the upcoming audit should focus on whether those same control procedures can allow sample sizes to be reduced.
- **Review of prior audit reports.** Significant past audit findings and their significance should be considered as well as the extent of management commitments to take corrective actions. To obtain leads to other sensitive areas, the auditor should also study reports on similar entities or functions in the organization. For example, if a branch-level audit is planned in a multibranch organization, recent internal audit reports covering other branches may point to potential problem areas in the branch planned for review. Related findings in other areas may also be useful.

  Particular workpaper review attention should be given if substantial corrective actions were required in that past audit, and the upcoming planned audit should include an examination of these areas as well. Internal audit should also review any disputed items from a prior report. Although internal audit management should have an objective of clearing up all disputed items in an audit report, there may be situations where the auditor and auditee agree to disagree. These internal audit reporting matters are discussed in Chapter 17. The auditor should note any such areas as a suggestion for a planned audit in an upcoming period.

- **Organization of entity.** The auditor should obtain an organization chart of the entity to be audited to understand its structure and responsibilities. In addition, the number of employees and the names of key employee contacts by major departments or sections should be obtained. Particular attention should be given to areas where there may be a potential separation-of-duties problem. This should include, if possible, the name of a key liaison person for contacts during the planned audit. If applicable, the entity's mission statement or similar functional descriptions should be obtained to better understand its purpose. Budgets and financial-performance data also should be reviewed as background material. An internal audit manager may want to gain this information through a telephone request or e-mail note and should advise the auditee that the requested information is to help in the planning of the potential audit. The areas reviewed when gaining an understanding of the entity's organization will vary somewhat depending on the type of audit planned. In an operational audit of a manufacturing area, for example, an internal auditor might want to gain an overall understanding of the manufacturing process. Similarly, a planned IT operations general-controls review would require the internal auditor to gain some background information about the operations environment, the telecommunications network, and the applications processed.
- **Other related audit materials.** Supporting data from related audits completed, planned, or in process should also be studied. These data may include problems identified by external auditors in a prior-period SOx Section 404 review or any reviews by governmental regulatory auditors. The results of internal reviews by departmental or other organization officials, press releases, and other related reports provide additional useful background material. Any indication of known problem areas from these reviews should be noted. In some instances, it is beneficial to review articles in the professional literature—such as the IIA's publications—to understand successful approaches used by other internal auditors.

7.3 Starting the Internal Audit

We have planned our internal audit at Global Computer Products and defined its objectives. Now a first step in starting the actual internal audit is to inform the group or organization to be audited—the auditee—that an internal audit has been scheduled. Although internal audit would have prepared a planning memo (Exhibit 7.1) as documentation for its own internal audit files, the function to be audited must be informed of this planned internal audit. The only exception to this rule would be a fraud-related investigation, where internal audit generally appears at the auditee site unannounced. (Fraud detection reviews are discussed in Chapter 25.) Otherwise, internal audit should inform appropriate persons at the facility to be reviewed through both an informal note followed up by a more formal notice.

This notice of a planned upcoming internal audit is called an engagement letter. It is an internal planning document that informs the auditee of *when* the internal audit is scheduled, *who* will be performing the review, and *why* the audit has been planned (a regularly scheduled, management, or auditor committee request, etc.). This who, what, and why approach should be used for all engagement letters. A

EXHIBIT 7.3 Internal Audit Engagement Letter Example

Global Computer Products

February 2, 20xx

To: Red Buttons, Dept. 7702
From: Lester C. Tuttle, Audit Supervisor
Subject: Accounts Payable Systems Audit

The internal audit department has scheduled a review of your purchasing systems and accounts payable processes. Our review will include internal controls over the key purchasing and accounts payable processes at Global Computer Products manufacturing facility at Minneapolis, MN. The review has been scheduled as part of our annual internal audit planning process, approved by the Board of Directors Audit Committee.

The objective of our review will be to assess the adequacy of purchasing system internal accounting controls at this Global Computer Products Minneapolis facility as well as the purchasing processes at multiple branch facilities, interfaces to the accounts payable system at corporate headquarters, and automated systems to support these processes.

Our audit is scheduled to begin on about March 15, 20xx with myself as the in-charge auditor, and two other members of the internal audit staff, Judy Spatz and Marcie Prusch, as well as Herman Hollerith who will lead a review of supporting network and IT systems controls. We plan to conclude our work in June, including the issuance of an internal audit report.

We will need access to your regular purchasing and accounts payable system records and files. In addition, please inform the vendors providing you with purchasing systems support that we may need to access some of their supporting systems as part of our internal audit testing.

Please arrange for systems access and temporary systems passwords for myself as well as our internal audit team of Spatz, Prusch, and Hollerith. We will also require some working space in your office area. Please contact me at lc.tuttle@globalcomputerprod.com or at ex 9999 if you have any questions.

L. C. Tuttle, Audit Supervisor
W. J. Rawdon, Audit Manager

sample engagement letter is shown in Exhibit 7.3. This letter should notify auditee management of:

- **Addressee.** The communication should be addressed to the manager directly responsible for the unit being audited.
- **Objectives and scope of the audit.** The auditee should be clearly advised of the purpose of the planned internal audit with the areas it will cover. For example, the letter might advise that internal audit plans to review internal controls over the shop-floor labor collection system, including main-plant shop-floor operations.
- **Expected start date and planned duration of the audit.** As much as possible, the engagement letter should give the auditee some understanding of the start and planned finish timing of the audit.

- **Persons responsible for performing the review.** At a minimum, the in-charge auditor should be identified. This will help auditee management to identify this key person when a team of auditors arrives on-site.
- **Advance preparation needs.** Any requirements needed in advance of the field visit or at the audit site should be outlined. This might include copies of certain reports. This is also an appropriate place to request internal audit temporary office space, telecommunications network access, and access to key IT systems or databases.
- **Engagement letter copies.** Although the term *carbon copy* or *CC* is outdated today, copies of the engagement letter should be directed to appropriate persons in the enterprise with a need to know.
- **Other operations reports.** Based on the overall audit objectives, financial, statistical, and other reports relating to the entity being audited should also be requested in advance as part of the engagement memo. Reports of this nature can help identify trends or allow comparisons between entities to determine any significant variances.

Appropriate levels of management should also be copied on this engagement memo. Although it is usually appropriate to inform auditee management that an internal audit has been scheduled, there may be circumstances where no formal engagement letter is released. For example, if the audit is fraud related, the review might be performed on a surprise basis and scheduled only through appropriate levels of senior management. Small retail locations, with a concern about cash controls, are also good candidates for surprise audits even though there is no suspicion of fraud. In most instances, however, auditee management should be informed of the planned audit visit and made aware of internal audit's planned objectives.

Some internal audit professionals have taken different stands on whether audits should be announced in advance. They argue that a surprise audit allows a review to see actual conditions without giving the auditee the benefit of cleaning up records, documentation, and other matters. However, the arrival of an audit team for an unannounced audit can cause some serious disruptions to an auditee organization, with the possibility that the prime auditee may be on vacation or away at a seminar. Unless there is a suspected fraud or a need for a surprise cash count, unannounced audits should generally be avoided. There may even be reasons to postpone or reschedule the review as announced in the engagement letter. For example, a key manager or technical support person may have a prescheduled vacation during the period of the planned audit. If that person is a key source of information and if there are no special reasons for the audit's planned time schedule, audit management should reschedule it to accommodate local management. In many situations, however, the unit management may inform internal audit that "this is a bad time," with no strong reasons for postponing the audit. Because internal audit has a comprehensive schedule of planned audits and its own scheduling problems, it is appropriate to refuse such requests for postponement and insist on initiating the audit as planned.

Once the audit has been scheduled and auditee management informed, the assigned audit team should be ready to begin work at the auditee site. This phase of the audit is called *fieldwork,* even though the audit may not take place at a remote site and possibly will just start down the hall from internal audit or will consist mainly of reviews through Web screens. The term *fieldwork* dates from earlier days when

internal auditors traveled to remote locations—the field—to perform their internal audit reviews. At this point, the internal audit team has gathered such background information as relevant policies and procedures. Internal audit would next perform a field survey to improve the assigned audit team's understanding of the areas to be reviewed as well as to establish preliminary audit documentation of those procedures. We are describing this internal audit field survey as a first-time audit event. However, in many cases, internal audit will be returning to perform a repeat review after a lapse of time.

(a) Internal Audit Field Survey

A preliminary survey is often critically important in determining the direction, detailed scope, and extent of the audit effort; it is the first step taken at the audit site. An internal auditor cannot just rush in with no clear purpose or objectives and begin examining documents and observing operations. A field survey allows auditors to: (1) familiarize themselves with the major local processes in place and (2) evaluate the control structure and level of control risk in the various processes and systems included within the audit. If members of the audit team are unfamiliar with the audit location and its management, this is the point to make introductions and to clarify any questions that may have been raised through the engagement letter. It is also the appropriate time for the in-charge auditor to outline planned interview requirements and to establish a preliminary schedule. These information elements should be assembled by the in-charge auditor and other members of the team during a typical field survey:

- **Organization.** During the field survey, the auditors should confirm that organization charts, including the names of key personnel, are correct. The auditor should become familiar with functional responsibilities and key people involved in the operations. Often a title on an organization chart does not reflect the true responsibilities of that position. Formal position descriptions should be requested whenever they may be appropriate. If the function does not have prepared charts available at the time of the preliminary survey, the auditor should draft a rough organization chart and review these assumptions with auditee management.
- **Manuals and directives.** Copies of applicable policy and procedure manuals, extracting data of interest for the audit workpapers, may be available through an online system, and appropriate access should be obtained. Applicable federal and state laws and regulations should be studied as well as management directives to comply with them. Depending on the overall objectives of the audit, correspondence files should also be screened for applicable materials.
- **Reports.** Relevant management reports and minutes of meetings covering areas appropriate to the audit—such as budgeting, operations, cost studies, and personnel matters, and the results of any external inspections or management reviews as well as actions taken—should be analyzed. Examples might include manufacturing cost performance reports or a fire inspector's review of an IT server center's physical security. Such reports may provide leads for the audit as well as a summary of problems faced, recommendations made, and progress made in their implementation.

- **Personal observation.** A tour or walk-through of the activity familiarizes internal auditors with the entity, its basic operations, personnel, and space utilization. It also provides the audit team an opportunity to ask questions and observe operations. Auditors are sometimes guilty of visiting an operation, spending much of their time in an accounting or administrative office, and completing the audit without a clear understanding of the actual activity audited. This can result in serious omissions in the final audit work. The impressions gained from this tour should be documented in the audit workpapers as a narrative. Compliance with company procedures should also be observed and documented.
- **Discussions with key personnel.** Discussions in the area being audited help to determine any known problem areas, the current results of the unit's operations, and any planned changes or reorganizations. Questions should be raised based on preliminary data reviewed or auditor tour observations.

The field survey should be the initial review contact point with the auditee; at this time, local management can meet the audit team, and the assigned auditors have their first exposure to the entity to be reviewed. Problems or misunderstandings can arise at this point. Although these matters should have been resolved at the time of the engagement letter release, unit management may not always understand what the internal auditors want, or internal audit may not have a correct understanding of the entity, despite preliminary planning. The result may point to a need somewhat to adjust the scope of the planned review, the planned audit procedures, or even the overall audit. Small changes are appropriate, but this is not the time to revise internal audit plans. If changes are requested, the assigned in-charge auditor should contact internal audit management for guidance.

This section has referred to both "the internal auditor" and "the in-charge auditor." Depending on the size of the overall internal audit staff and the audit engagement, the review may be performed by one or several internal auditors. One assigned auditor should always be designated as the "in-charge auditor," with responsibility for making most on-site audit decisions. In-charge responsibilities usually are assigned to more senior members of the audit staff, but the responsibility can be rotated throughout the staff to give less experienced auditors some management experience. Internal audit staffing roles and responsibilities are discussed in Chapter 12.

(b) Documenting the Internal Audit Field Survey

Normally, the field survey will occupy the first day or two at the audit site. For large reviews, the survey can be performed during a separate visit in advance of the auditor's detailed testing and analysis work. In either case, the work performed and summaries of data gathered through the field survey should be documented in audit workpapers. Copies of key reports and published procedures should be obtained, summary notes and observations recorded from all interviews and tours, with flowcharts prepared for all systems or processes. These materials will be part of the auditor's workpapers, as discussed in Chapter 16.

An internal auditor's field survey also can identify new or revised audit techniques in the light of changed procedures or operating conditions. For example,

functions that were once traditional IT application processes may now be Web-based. Flowcharts should be prepared to describe major processes including changes from any prior audits. Through their graphic summary of the operations and data, flowcharts are often a key tool to illustrate the complexities and control points in a system or process. The old adage that "a picture is worth a thousand years" very much applies here.

Developing flowcharts for all major transaction processes is important for documenting many internal audit process and is essentially necessary for the SOx Section 404 documentation discussed in Chapter 4. There are many variations and approaches to developing flowcharts, and they are good tools to show the relationships between different operational elements and where control points exist in a process. Once completed, these flowcharts become part of the auditor's permanent workpaper file for that entity. They also support requirements that organizations maintain documentation covering their internal controls. The ability to construct an effective process flowchart should be part of every internal auditor's CBOK.

(c) Field Survey Auditor Conclusions

The purpose of an internal audit field survey is to confirm the assumptions gained from the preliminary audit planning, in order to develop an understanding of key systems and processes. Because the information that supports the preliminary audit planning is often imperfect, this is an important point where the assigned audit team can make adjustments to the planned audit scope and objectives. For larger audits, it is often a good idea for internal audit management to visit the team performing the field survey and review its results. This way, any necessary management-approved scope changes can be made. This on-site presence can clear up any questions that could be raised later.

An internal auditor may encounter instances where the information gathered from a field survey may cause the audit team either to adjust the planned audit scope substantially or even to cancel the detailed audit work. Sometimes the audit team involved in the preliminary planning may call the auditee at a remote location and be advised that there are "no changes" in the area of the auditor's interest. When the audit team arrives, the field survey could point out significant changes, such as the introduction of a new information system that changes the overall control environment and may require the internal audit team to add another specialist to the project, causing both staffing and audit test strategy adjustments. In other cases, the audit team may find that changes are so substantial that the planned audit should be canceled or postponed. In most instances, however, the field survey provides the audit team with additional data to help it adjust its planned procedures.

The materials gathered in an internal audit field survey should be used either to document or to update a workpaper permanent file. If a member of audit management is not on-site, the results of the survey should be summarized in written form, communicated through e-mail, and reviewed with internal audit management before proceeding with the audit. Exhibit 7.4 is an example of an internal audit report on field survey conclusions. This document is particularly important if the in-charge auditor feels there is a need to change audit scope or planned procedures.

EXHIBIT 7.4 Field Survey Conclusions Audit Report Example

April 1, 20XX

To: Sandra Smyth, Audit Manager
From: Lester Tuttle
Subject: Purchasing and Accounts Payable Minneapolis Field Survey

We have concluded our field survey at the Minneapolis site that included a review of active supporting processes as well as an observation of operations. While most of our preliminary internal audit plans to review internal controls are correct and will support our upcoming planned internal audit here, we identified several areas where our planned audit scope and planned procedures should be modified:

1. *Cash Discount System.* We were advised that with the low interest rates we have been experiencing in recent years, the unit has found little advantage in taking cash discounts from prompt payments. As a result, we were advised that these processes are not normally used today. We should modify our planned audit procedures in this area from the planned 20 hours to just a very limited 4-hour internal audit documentation update.
2. *Prevalence of Web-Based Processes.* Local purchasing systems have moved from the more paper-forms-based processes of just five years ago to a totally Web-oriented environment. Our planned hours should be expanded to document these new processes and to develop new testing procedures as appropriate. Hermann Hollerith was budgeted for 145 hours over three months to review and test the old system. We should expand his planned 145 hours to 200 hours with his planned 20 hours in the first month expanded to 40 hours. That time would be spent on understanding, documenting, and developing testing procedures for the Web application.

Please advise if these proposed changes to our audit plan here are acceptable.

Lester C. Tuttle

7.4 Developing and Preparing Audit Programs

Internal audits should be organized and performed in a consistent manner with an objective of minimizing arbitrary or unnecessary auditor procedures. To achieve audit consistency, internal auditors should use what are called *audit programs* to perform audit procedures in a consistent and effective manner for similar types of audits. The term *program* refers to a set of auditor procedures similar to the steps in a computer program, instructions that go through the same program instructions every time the process is run. For example, a computer program to calculate pay will include instructions to read the time-card file of hours worked, look up the employee's rate stored in another file, and then calculate the gross pay. The same steps apply for every employee unless there are exceptions, such as overtime rates, coded into the payroll program. Similarly, an audit program is a set of preestablished steps an internal auditor performs. An audit program is a tool for planning, directing, and controlling audit work and a blueprint for action, specifying the steps to be performed to meet audit objectives. It represents the auditor's selection of the best methods of getting the job done and serves as a basis for recording the work steps performed.

An effective internal audit department should have a series of generalized audit programs prepared for most of its recurring audit activities. Many of these programs,

such as one covering an observation of the taking of physical inventories, are used from year to year and enterprise entity to entity with little change. In other situations, the internal auditor may have to modify a standard program to the unique aspects of a particular audit. In some situations, a standard audit program will not be applicable. For example, an internal auditor may want to review controls in a new business entity with some unique control characteristics, or audit management may want to take a different approach because of problems encountered with similar previous reviews. Based on planned audit objectives and data gathered in the preliminary and field surveys, the in-charge auditor may want to prepare a customized audit program for guiding the review. This may be little more than a standardized program with minimal local changes, or it may be a unique set of audit procedures based on the preliminary planning and the results from the field survey. In order to prepare this program, the internal auditor first should have an understanding of what constitutes an adequate audit program.

(a) Audit Program Formats and Their Preparation

An audit program is a procedure describing the steps and tests to be performed by an internal auditor when actually doing fieldwork. The program should be finalized after the completion of the preliminary and field surveys and before starting the actual audit. It should be constructed with several criteria in mind, the most important of which is that the program should identify the aspects of the area to be further examined and the sensitive areas that require audit emphasis.

A second important purpose of an audit program is that it is a tool to guide both less and more experienced internal auditors. For example, management may request that internal audit observe the taking of an annual physical inventory. This type of review consists of fairly standard procedures to assure, among other matters, that goods shipping and receiving cutoff procedures are proper. A less experienced internal auditor may not be aware of these procedure steps, and even experienced internal auditors may forget one or another. An audit program outlines the required audit steps. An established internal audit department probably will have built a library of audit programs, established over time, for tasks such as a physical inventory observation or a review of fixed assets. When planning a review where such established programs exist, audit management needs only to use these programs with consideration given to any changed conditions that have been discovered through the preliminary or field surveys. The audit program then is revised as necessary, with the changes approved by audit management prior to the start of the review.

For many internal audit departments, appropriate established audit programs may not be available for some areas. This is because internal auditors typically face a wide and diverse set of areas for review, but they will not have the time or resources to review every area frequently. Established programs prepared for prior audits often become out of date due to new systems or changed processes. The internal auditor responsible for the field survey or another member of audit management should update any existing audit program or prepare a revised set of audit program steps for the planned review. Depending on the type of planned audit, programs usually follow one of three general formats: (1) a set of general audit procedures, (2) audit procedures with detailed instructions for the auditor, or (3) a checklist for compliance reviews.

EXHIBIT 7.5 General Audit Program Instructions for Direct Expenditures

Step	Internal Audit Procedure	W/P Ref.
1	Determine that valid/authorized purchase orders exist for each purchasing transaction.	
2	Duplicate purchase orders should not exist and not be processed.	
3	Open/outstanding purchase orders should be investigated and resolved.	
4	Receipts of goods should be processed and recorded only once.	
5	Receipts of good should be processed and recorded only if a valid purchase order exists.	
6	Vendor invoices are processed and recorded only for goods ordered and received.	
7	Vendor invoices are processed and received only once.	
8	Debit memos are generated only for real/authorized transactions.	
9	All receiving transactions are processed and recorded in the proper period.	
10	Purchase orders contain accurate price, units of measure, and other relevant data.	
	Signature Date	

Several examples here illustrate these audit program types. Exhibit 7.5 is a general audit program for a review of the direct expenditure cycle, the product-related purchase process in an enterprise. The program outlines the high-level or general audit steps that internal auditors will need to follow when performing internal audits in that area. With a library of such high-level audit programs covering reviews of each major business cycle, such as direct expenditures, fixed assets, and others, internal audit needs to tailor these general audit programs to the specific unit under review. Often internal audit will take its general audit programs and tailor them to more specific areas.

Exhibit 7.6 is an example of a more detailed audit program; covering audit steps for a review of petty cash controls at a branch unit. It consists of general audit procedures to review cash at any unit of a multifacility organization. Petty cash controls are one of the smaller, less critical internal control concerns for many enterprises, and an internal auditor often performs this type of review regularly. Internal audit sometimes makes these types of detailed audit programs even more specific or detailed. The program shows the steps that should be included in any such audit and illustrates an example audit program.

Exhibit 7.7 represents a typical internal audit program format where audit tasks are broken into numbered steps with space allowed for the initial and date of the internal auditor completing the audit step as well as a column for a reference to the workpaper that describes the audit step. For example, for the step 1 start of this process, the internal auditor performing the procedure would document cashier responsibilities. Typically, an established internal audit function would have developed these types of audit programs for many of its regular audits. The audit team visiting an organizational unit could then use standard programs to review internal controls in a consistent manner from one unit to the next. This is particularly important in a multi-unit organization where audit management wants to have assurance that controls over the area were reviewed and evaluated in a consistent manner,

EXHIBIT 7.6 Audit Program Standard Format: Review of Petty Cash

Audit: _____ Location: _____ Date: _____

#	Audit Step	Initial & Date	W/P Ref.
1	Prior to review, determine who is the cashier responsible for the petty cash fund balances,receipt requirements, replenishment procedures, and guidelines for authorized disbursements.		
2	Perform this petty cash review on a "surprise" basis. Identify yourself to cashier, request that the cashier function be closed but observe audit during your initial review, and make a detailed count of cash in the account as well as any included personal checks.		
3	Having performed count in presence of cashier, ask cashier to acknowledge results of the auditor's cash count.		
4	If any personal checks found in the cash count were over one day old, ask why they were not deposited or if they are being held as collateral for an employee short-term loan fund. If such a fund, assess propriety of this practice.		
5	Reconcile the audited cash count with the fund's disbursement register, noting any differences.		
6	Determine that all cash disbursements recorded have been made to valid employees for authorized purposes.		
7	Observe office security procedures covering the fund and determine that funds are locked or otherwise secured.		
8	Review procedures for fund replenishments. Select a prior period, review its supporting documentation, and reconcile activity to purchase journal.		
9	Assess the overall control procedures, propriety, and efficiency of this petty cash process. Comment as appropriate.		
10	Determine that the petty cash function is used only for authorized small cash disbursements rather that a general change or short term loan fund.		
11	Document the results of the review and take steps to initiate immediate corrective actions if any problems were encountered during this review.		
12			

Signature Date

no matter who the assigned auditor or the location. This sample audit program is shown as a printed document that could be developed and controlled by internal audit. Of course, this would be a document located in the auditor's laptop system. In some instances, the in-charge auditor might prepare a custom program to evaluate certain special procedures encountered during the field survey.

The checklist-format audit program was once internal audit's most common format. Often junior internal auditors would be given an audit program composed of a long list of questions requiring "yes," "no," or "not applicable" responses and would complete these program steps either through examinations of documents or through interviews. Exhibit 7.7 is an example of a checklist-format audit program for reviewing ethics and business compliance policies. Yes-and-no responses, when asked in an information-gathering context, are often appropriate. A checklist-format

EXHIBIT 7.7 Checklist Format Audit Program: Review of Business Ethics

#	Internal Control Concern	Yes	No	N/A
1	Does the enterprise have a written code of business ethics/business conduct?			
2	Is the code distributed to all stakeholders?			
3	Are new stakeholders/employees provided an orientation for the code?			
4	Does the code assign responsibilities to operating personnel and others regarding compliance with the code?			
5	Are all stakeholders required to acknowledge that they have read, understand, and agree to abide to the Code?			
6	Are training programs delivered to all stakeholders regarding compliance with the code?			
7	Does the code address standards that govern personnel conduct in their dealings with suppliers and customers?			
8	Is there an effective mechanism in place to allow employees and other stakeholders to confidentially report suspected violation of the code?			
9	Are there appropriate mechanisms in place to follow up on reports of suspected violations of the code?			
10	Is there an appropriate mechanism to allow employees and other stakeholders to find out the results of their reported code-related concerns?			
11	Is compliance with the code's provisions a standard used for measuring personnel performance at all levels?			
12	Is compliance with the code's provisions a standard used for measuring employee and stakeholder performance at all levels?			
13	Is the code consistent with the requirements of the Sarbanes-Oxley Act?			
14	Are there procedures in place to update the code on a regular and periodic basis?			
	Signature Date			

audit program has two weaknesses, however. First, while a series of auditee yes-or-no type interview responses can lead an experienced auditor to look at problem areas or to ask other questions, less experienced auditors may miss problems when just completing the questionnaire and not digging a bit deeper. A procedures-oriented audit program better encourages follow-up inquiries in other areas where information gathered may raise questions.

The questionnaire-format audit program also tends to cause auditors to miss examining necessary evidential matter when only asking the questions. An inexperienced internal auditor can too easily check "yes" on the questionnaire without determining, for example, whether that response is properly supported by audit evidence. An example would be a question regarding whether some critical document is regularly approved. It is easy to ask the question, receive an answer of "yes," and never follow up to see if those documents actually were approved. Each of these audit program formats will work for different types of reviews, provided the internal auditor gives some thought to the program questions. The key concern is

that all audits should be supported by some type of audit program that documents the review steps performed. This approach allows audit management to recognize what procedures the auditors did or did not perform in a given review. Strong and consistent audit programs are an important step in improving the overall quality of the internal audits performed.

The reliability of the planned materials and processes to be reviewed and internal audit's other understandings about an operation should also be considered when developing an audit program for a specific facility or resource. There is little value in developing an audit program at a facility that calls for a review of systems and procedures when they are no longer in use. An internal auditor, in developing an audit program, should try to select audit steps that are meaningful and that will produce reliable forms of audit evidence. For example, the audit program often needs to call for detailed tests in a given critical, high-risk area rather than suggesting that the information can be gathered through interviews.

Advanced audit techniques should also be incorporated into audit programs wherever practicable. For example, computer-assisted audit tools and techniques (CAATTs), discussed in Chapter 21, can perform selected audit steps. The use of procedures such as statistical sampling allow an internal auditor to extract data easily from larger populations. Members of the audit staff who have IT audit or other technical skills should be consulted when preparing these audit program steps. There is no single best format for an audit program; however, the program should be a document that auditors can use to guide their efforts as well as to record activities. That audit program will then be included in the workpapers to serve as almost a table of contents of the audit activities performed.

(b) Types of Audit Evidence

As discussed in Chapter 8, the IIA professional standards state that an internal auditor should examine and evaluate information on all matters related to the planned audit objective. This information, called *audit evidence,* covers everything an internal auditor reviews or observes. The internal auditor should gather audit evidence in support of the auditor's evaluation—what internal audit standards call *sufficient, competent, relevant,* and *useful* audit evidence. A properly constructed audit program should guide an internal auditor in this evidence-gathering process. However, multiple types of evidence can be useful in developing audit conclusions. If an auditor actually observes an action or obtains an independent confirmation, this is one of the strongest forms of evidence. However, a casual response to an auditor's question covering that same area will be weaker. It is not that an auditor thinks the auditee is not telling the truth, but actually observing some event is far superior to just hearing about it. Internal auditors will encounter different levels of audit evidence and should attempt to design their audit procedures to look for and rely on the best available audit evidence. Exhibit 7.8 provides some ranges of best evidence for different classifications of materials. The idea that a written, signed document is better evidence that a casual response should be no surprise to an internal auditor, but it is always good to keep these concepts in mind.

The field survey and the subsequent development of an audit program are preliminary activities to performing the actual internal audit. It is often more efficient to have supervisory personnel complete these preliminary steps before assigning staff auditors for the actual review. These supervisory auditors, either audit management

EXHIBIT 7.8 Internal Audit "Best Evidence" Classifications

Evidence Classification	Strongest	Weakest
Audit technique	Observation/confirmation	Casual inquiry
Origin of the evidence	Corroborative materials	Underlying statistics
Relationship of the auditee	External document	Auditee internal document
Form of audit evidence	Written with signatures	Oral comments
Sophistication of evidence	Formal documentation	Informal such as notes
Location of evidence	Connected to area reviewed	Derived/supporting materials
Source of audit evidence	Product of internal audit work	Other supporting materials

or experienced in-charge auditors, usually have the experience to make quick assessments of field situations and to fine tune the overall audit approach. Once the survey and the completed audit programs have been reviewed and approved by internal audit management, the next challenge is performing the actual internal audit to meet its desired audit objectives. The preparatory work from the survey will play an important role in assuring the audit's success; however, the internal auditor is now faced with the day-to-day problems of performing the actual audit.

The audit steps performed here will depend on the characteristics of the entity audited. A financially oriented audit of a credit and collection function will be quite different from an operational review of a design engineering function. The financial audit might include independent confirmations of account balances; the operational audit typically includes extensive interviews with management and supporting documentation to assess key internal controls. Despite these differences, all internal audits should be performed and supervised following a general set of standards. This will ensure that internal audits are properly directed and controlled.

7.5 Performing the Internal Audit

This section discusses general steps necessary to perform any internal audit and should be used in conjunction with other specific audit procedures discussed throughout this book. Understanding how to perform an internal audit is a key CBOK requirement. While the previously discussed preliminary survey is an important planning step, an engagement letter, shown in Exhibit 7.3, is the important first step in announcing a planned audit and defining its objectives and scope, the assigned audit team, and the approximate time periods. A single engagement letter is usually sufficient; however, in some audit situations, there may be a considerable time interval between an initial field survey and the actual audit. A second engagement letter then would then be useful.

An engagement letter outlines the arrangements for the planned internal audit. As discussed, unannounced audits may be justified in cases where there is a suspicion of fraud or when a unit is very small, with records that can be easily altered. In most instances, however, audit management should start the review with this formal engagement letter that alerts local and line management of the planned review, allowing them to adjust their schedules as appropriate. In some instances, auditee management may request a postponement due to any number of reasons. With the exception of a potential fraud situation, internal audit management should always try to be flexible here.

The assigned internal auditors also have some advance work prior to actual fieldwork. If there was a separate field survey, those results should be reviewed, as should any past audit permanent file workpapers. For larger audits with multiple assigned auditors, audit area responsibility assignments should be made in advance. Travel and lodging arrangements should be made in accordance with organization policies. Travel costs can be a major expense for an internal audit department, particularly if there are numerous, scattered audit locations, either domestic or worldwide. Often significant travel savings can be realized by taking advantage of discount airfares and making other cost-effective travel arrangements. Internal audit management must recognize, however, that travel always will be a major budget expense and should not eliminate trips to higher audit-risk locations just because of the cost of travel. Internal audit has a responsibility to the audit committee and senior management to report on the status of the organization's internal control structure. Field visits should not be postponed or eliminated just because of the cost of travel to remote locations.

(a) Internal Audit Fieldwork Initial Procedures

An internal audit can cause interruptions and problems in the day-to-day operations of the auditee organization. The in-charge auditor and members of the audit team should begin by meeting with appropriate members of auditee management to outline preliminary plans for the audit, including areas to be tested, special reports or documentation needed, and personnel to be interviewed. This also is an appropriate time for the internal audit team to tour and meet other personnel in the unit to be reviewed. The auditors should request that management contact all affected members of the auditee organization to provide them with an auditor-prepared tentative schedule of the planned audit work. This will eliminate potential problems in securing the cooperation of auditee personnel.

Despite the best of plans, problems still can occur while conducting the audit. For example, a key department supervisor may claim to be too busy to talk to internal audit and will not supply necessary information. Similarly, a cycle from a key computer system file that was to have been saved for audit tests may have been deleted. These types of problems can either slow progress or require a revised testing and analysis strategy. Any problems should be detected early in the assignment and solved as soon as possible. Difficulties in obtaining cooperation of one department's personnel, for example, may slow work in that area and delay the completion of the entire audit.

The in-charge auditor should meet with auditee management to discuss any problems and to find solutions. If local management appears to be uncooperative, the in-charge auditor may have to contact internal audit management to resolve the problem at a different level. If a key component of the planned audit is missing, audit management should develop a revised strategy to get around the problem. This might include:

- Revising audit procedures to perform additional tests in other areas. This type of change, however, must be performed with care. If there was a strong reason for selecting the now-missing file—such as the need to tie it to some other data—it may be necessary to reconstruct the missing balances.
- Completing the audit without the missing data file. The workpapers and the final report would indicate internal audit's inability to perform the planned tests. The

in-charge auditor should always gain approval from internal audit management for this approach.

- Complete other portions of the audit and reschedule a later visit to perform tests. (This is only an option if the missing data file cannot be reconstructed or if a different cycle of data would not be sufficient. Management should be informed, of course, of audit budget overruns because of this problem.

These or similar problems can be encountered. It is important that such problems be detected and resolved as early in the audit as possible. If the internal audit team faces a total lack of cooperation, management at appropriate levels should be informed to resolve the matter. Both the internal auditors and auditees should remember that both parties are members of the same overall enterprise with common general interests and goals.

The actual audit fieldwork should follow the established audit program. As each step is completed, the responsible auditor should initial and date the audit program. Documentation gathered from each audit step, as well as any audit analyses, should be organized and forwarded to the in-charge auditor to perform a preliminary review of the audit work. The in-charge auditor monitors the performance of the audit work in progress and reviews workpapers as they are completed for each step. Exhibit 7.9 shows a field audit workpaper point sheet where the in-charge auditor has signed off on key audit program steps and suggested areas for additional work. The comments from this sheet go back to our Exhibit 7.6 audit program for a review of petty cash. Of course, we are using petty cash as an example even though it is usually a relatively small, low-risk area; this type of point sheet document is a useful example for all larger audits.

EXHIBIT 7.9 Internal Audit Workpaper Review Point Sheet Example

Workpapers Reviewed: ***Review of Petty Cash at Columbus Office on yy/mm/dddd***
Auditor: ***Marcie Prusch***
Workpaper Reviewer: ***Lester C. Tuttle***

Step	Audit Procedure	Reviewer Comments	W/P Ref	Initials
1	Determine cash review responsibilities.	*OK.*		
2	Perform surprise cash count.	*No indication if any personal checks we found in surprise cash count.*		
3	Obtain cashier acknowledgement.	*OK.*		
4	Review personal checks in account.	*This step is missing from W/P's.*		
5	Reconcile audited cash to disbursement register.	*No indication in W/P's the accounts are in balance.*		
6	Determine if disbursements were to authorized persons.	*OK.*		
7	Observe office security procedures for fund.	*Description limited—should be expanded.*		

Note: Sample workpaper review notes from the first steps of a petty cash review from Exhibit 7.6.

Point sheets should always be supported by and cross-referenced to the specific audit workpapers, and the status of the points or issues raised should be documented to show their eventual disposition. If developed into a finding, the point sheet can also be cross-referenced to that audit report finding. If the point-sheet potential finding is dropped by the internal audit team during the fieldwork or later, the reasons should be documented. The results of many audit steps will not yield specific audit findings but may raise questions for further investigation. The conditions in many areas reviewed can be subject to explanations or interpretations by local management. Rather than just writing them up, the field audit team should generally discuss their preliminary audit observations with the persons responsible for the area. An auditor sometimes can misinterpret something that is easily resolved. If questions still remain, the matter may become a preliminary audit finding, as discussed in the next section.

(b) Audit Fieldwork Technical Assistance

The field survey or the audit program development process should have identified any need for specialized technical help to perform the audit; however, other complex problems requiring technical support may arise in the course of the audit fieldwork. For example, the assigned auditor may question the accounting treatment of a certain set of transactions and want to get better information about normal practices for them. Similarly, internal auditors may encounter a specialized IT application, with unique control considerations, that was not sufficiently described in the survey.

If a technical issue is not familiar to the audit team, the in-charge auditor should seek assistance as soon as possible. An internal audit supervisor or specialist may have to research the audit or technical issue in order to provide the answer. In other instances, it may be necessary to bring an internal audit expert in the area in question to the field site to resolve the problem. However, a typical internal audit department does not have resident experts ready to travel out to the field site to resolve a problem, and issues can normally be resolved through telephone calls or e-mails.

The important message here is that internal audit management should communicate to its staff is that all technical audit problems should be brought to the attention of the in-charge auditor for resolution as soon as possible. Any cost and extra time requirements caused by these technical problems should be documented. If the technical problem cannot be resolved promptly, it may be necessary to reschedule the audit or to revise the strategy, as described.

(c) Audit Management Fieldwork Monitoring

If the internal audit covers an extensive period of time or level of required resources, internal audit management should review an audit's progress frequently and provide technical direction through visits and communications. These reviews supplement the ongoing work of the in-charge auditor, who is part of the field staff. The frequency and extent of these visits will depend on the criticality of the review, the experience of the assigned staff, and the size of the review. A medium-size review headed by an experienced in charge auditor and covering familiar areas may not require a management review if communication lines are good. However, if the audit covers a critical area, if a new program or new techniques are used, or if the assigned in-charge auditor has limited experience in the area reviewed, an experienced member of audit management should visit the fieldwork project periodically.

The purpose of these visits should be to review the work in progress and to help resolve any problems encountered. While audit management sometimes may feel that this is also an appropriate time to take the assigned field staff out to lunch or dinner to thank them for their efforts, everyone should realize this is not the purpose of audit field visits. Audit management should take this opportunity to understand any evolving issues in the audit and to suggest changes as appropriate. This is also a good time for management to start the review of completed audit workpapers, as discussed in Chapter 16.

Internal audit workpapers document the work performed and provide a link between the procedures documented in the audit program and the results of audit tests. Because they will become the basis for findings and recommendations in final audit reports, the workpapers should document all audit work. While the in-charge auditor should have been reviewing and commenting on workpapers for larger audits through audit point sheets as illustrated in Exhibit 7.9, smaller reviews with a limited audit staff will not always have this type of feedback. Point sheets are an internal audit quality assurance measure and should be used by the audit team as a measure to bring issues to the attention of both internal audit and auditee management early in the review. They also serve as a control to ensure that all leads are followed up. In addition, the various auditor point sheets, developed by individual staff members, may bring out a number of minor issues that fall into a pattern, indicating a more serious overall condition.

The member of audit management visiting the field site should spend some time reviewing and approving the workpapers and preliminary finding sheets. These workpaper-review comments should be documented, cover such areas as additional work or explanations required, and suggest adjustments to the audit program if appropriate. The management review typically should not result in major changes to the audit approach. However, internal audit management often can bring some additional guidance or understanding to the audit in process.

The review comments should be documented in a manner that references the workpapers when the management reviewer has questions or identifies missing items of audit documentation. Based on these review comments, the staff auditors should perform the additional audit work required and make necessary changes to the workpapers, indicating the action taken on the review sheet. After completion of internal audit's comments, the additional work done, or corrections, the supervisor indicates on the review comment sheets his or her clearance of all items as well as any further actions to be taken.

(d) Potential Audit Findings

Whenever an internal auditor discovers a potential audit deficiency, a brief summary of the conditions found and potential findings and recommendations should be prepared. This summary is sometimes called an *audit preliminary findings sheet.* Based on the Exhibit 7.3 engagement letter and partially on the general audit program steps outlined in Exhibit 7.5, Exhibit 7.10 is an audit preliminary findings sheet for our sample audit of accounts payable processes for Global Computer Products operations in Minneapolis. Whether the conditions described in such a preliminary document result in the final audit report finding depends on the results of additional review and analysis. These preliminary findings describe deficiencies or opportunities for improvement that were identified during the audit. Preliminary findings may have been developed through the auditor point sheets, described earlier, or through

EXHIBIT 7.10 Preliminary Audit Findings: Purchasing and Accounts Payable Audit

Global Computer Products

April 15, 20xx

To: Workpaper Files
From: L. C. Tuttle, Audit Supervisor
Subject: Purchasing and Accounts Payable Systems Audit Preliminary Findings

This memo is to document our preliminary observation from our recent review of the key purchasing and accounts payable processes at Global Computer Products manufacturing facility at Minneapolis, MN. The objective of this review was to assess the adequacy of purchasing system internal accounting controls at the Global Computer Products Minneapolis facility as well as the purchasing processes at multiple branch facilities, interfaces to the accounts payable system at corporate headquarters, and automated systems to support these processes.

Our preliminary findings and observations from this review are listed below. The observations may be subject to revision based on management comments or clarification regarding our observations. In addition, these observations will be supported by a full internal audit report to be issued on about May 5, 20XX.

While we found internal controls and procedures to be generally adequate, we observed the following areas requiring corrective actions:

1. Valid purchase orders were missing for some equipment in the new products engineering laboratory.
2. Existing policies for investigating open purchase orders are not being followed and we observed a growing number of these documents.
3. Purchase orders issued for materials in the Speedo division were frequently missing part units of measure—creating an environment for potential errors.
4. The new Web-based purchasing system is lacking daily input balancing controls—creating an environment where duplicate purchase orders could be issued.
5. Purchasing and accounts payable records and systems are not regularly included in the new corporation business continuity plan.

L. C. Tuttle, Audit Supervisor
W. J. Rawdon, Audit Manager

other internal audit documented findings and observations. These items start the preliminary report-writing process early in the audit and help to ensure that the essential facts for developing an audit report finding have been obtained. Although the contents of a preliminary audit finding can vary depending on the needs of the particular internal audit, preliminary audit findings typically have these elements:

- **Identificatio of the finding** This is just an identification number for the audit and a description of the potential findings.
- **Conditions.** The description here should be brief but sufficient to give local management an understanding of the conditions found.
- **References to the documented audit work.** The audit point sheet should contain cross-references to the step in the audit program that initiated the comment, as well as where it is documented in the audit workpapers.

- **Auditor's preliminary recommendations.** Audit report space should be used to document the nature of the potential audit finding, and what was wrong. This might become the basis for a potential future audit report finding. Some notes on potential auditor-recommended corrective actions might be included here.
- **Results of discussing the findin with management.** The in-charge auditor should discuss all potential findings on an informal basis with the manager directly responsible for the matter. The results of this conversation should be documented here.
- **Recommended disposition of the matter.** On the basis of the conversation with management, the in-charge auditor should include comments on the recommended disposition of the finding. It might be recommended for inclusion in the audit report, dropped for a variety of reasons, or deferred until more information can be gathered.

(e) Audit Program and Schedule Modifications

The audit program is the overall guide for conducting an internal audit. Developed from preliminary survey data and from any past internal audits on file, they may be subject to adjustment during the course of the review. Auditors must be responsive to new evidence, changes in supporting systems, and other changes in conditions. In the early stages of an audit, it may be necessary to redirect some of the planned staff assignments as well as to modify some audit program steps. Of course, the in-charge auditor in the field always should obtain approval from audit management before making any such changes.

The need for audit program modifications is most common when internal audit has developed a common audit program for use in reviews of similar but not identical units. For example, an audit program may have been developed to cover internal controls over the purchasing function for an organization with multiple independent manufacturing units, each with separate purchasing functions. Those purchasing function audit programs should reflect both organization policy and general internal control principles. Due to local differences, however, this audit program may contain steps that are not applicable to one or another specific purchasing area under audit. Any such steps that are bypassed on the individual audit program should be approved and documented as to the reasons.

Changes often are required in the audit schedule as work progresses, and some flexibility should be factored into plans to meet unforeseen requirements. During the field audit assignment, situations may be encountered that affect the progress of the audit, such as an unexpected problem or event, the need to modify or drop an audit program segment, the discovery of a new area for review, or changes in audit personnel. In other instances, there may be slippage in the plan due to additional time requirements to finish an audit program step. In these circumstances, revised budgets often are needed. Proper approvals for these changes always should be obtained from internal audit management.

(f) Reporting Preliminary Audit Findings to Management

A major area of emphasis in any internal audit is the identification of areas where the unit reviewed is not in compliance with good internal control procedures and where improvements are needed. These areas would have been documented during

the course of the audit through the use of point or findings sheets and preliminary findings types of documents. Although these potential audit items should have been discussed with the unit supervisors directly responsible, the audit team also should review them with unit management before leaving the field audit assignment.

Potential audit findings should be reviewed with unit management during the audit to determine if they are factual and appear to be significant. Depending on the scope and size of the audit, these potential findings should be reviewed at several points during the course of the review. If an audit is scheduled over multiple weeks, the in-charge auditor might schedule a meeting with unit management at least at the end of each week to discuss all findings that developed over the course of that week. If the findings are of a minor, procedural nature, management can take necessary corrective actions at once. They can then be deemphasized or deleted in any final audit report. For other findings, the in-charge auditor should review proposed findings to ascertain that cost savings are indicated and properly reported and that findings are related to operational effectiveness.

Even though the audit's duration may be too short to have weekly status meetings, the field audit team should review all potential findings with unit management before leaving the location. This will allow internal audit to present its preliminary findings and recommendations to local management to obtain their reactions and comments. It also gives both parties an opportunity to correct any errors in the preliminary audit report findings before internal audit leaves the location.

7.6 Wrapping Up the Field Engagement Internal Audit

Internal audits should be managed in the same manner as any large project requiring personnel time and other resources and resulting in a defined deliverable. Both personnel resources and other costs should be planned and budgeted on a detailed level. Chapter 14 talks about project management for internal auditors. The audit's actual performance should be recorded and measured against established time- and cost-based budgets to analyze and correct for any significant variances. Significant project milestones, such as the completion of fieldwork or the draft audit report, should also be tracked against plans. Of course, the most important internal audit work product is the formal audit report, along with its findings and recommendations, which is delivered to the auditee after completion of the review as well as to the audit committee. The internal audit reporting processes, as well as some sample audit reports, are discussed in Chapter 17.

Chapter 15 discusses audit planning and the development of the annual audit plan while this chapter considers the need for detailed plans for individual audit projects. Individual internal audits should be budgeted with time and other costs measured against those plans. No matter how large or small an enterprise's internal audit function, an audit project performance-reporting system should be established. For audits greater than about two weeks' duration or those performed in multiple locations at the same time, progress reports should be required on a weekly or biweekly basis. These reports should be based on the time summaries from the assigned audit staff as well as commentaries from the in-charge auditor at the location. They can include such information as budgeted and actual time to date, estimated time to complete, and a summarized description of progress against the

audit program. These data can be gathered by the supervising auditors at field sites and transmitted to the central internal audit department. The in-charge auditor should take responsibility for explaining any significant variances in audit actual versus budget performance. Such a report would be based on an overall internal audit time reporting system that measures expended staff internal audit hours against established internal audit budgets.

The time expended on individual audit projects should be further summarized by internal audit management to provide an overview of all audits planned or in process. A three-month period is often a good time period for planned future activities, given the various senior management requests and other factors that can impact an internal audit plan. This type of report is used to provide control over audits scheduled or in process while a separate, more detailed report can be completed for each individual audit to ensure that they are started and completed on a timely basis. The rolling three-month report can be a useful tool for communicating with the audit committee.

Any increases in audit time budgets should be monitored carefully, identifying reasons for the variance as well as any corrective action plans. Audit project monitoring should indicate any audits not started on time or that are outside of budget parameters. In some cases, the problem may be inaccurate budgets; in others, the problem may lie in auditor performance. Close control of the audit will prevent slippage caused by inadequacies in staff, delays in solving problems, insufficient supervision, and excessive attention to detail.

As discussed in Chapter 14 on project management for internal auditors, automated tools should be developed and maintained for an internal audit reporting and control system. Spreadsheet or database packages can provide a powerful structure for building such systems. Many paper-based reports can be eliminated, and the field auditors can transmit their time summaries and status report information to a central internal audit project-reporting system.

7.7 Performing an Individual Internal Audit

As is discussed throughout this book, internal auditing is a large and complex process with many activities. The concept behind our CBOK theme is to highlight the knowledge areas that are important to any internal auditor. While the internal audit reports discussed in Chapter 17 are internal audit's most import work product, the ability to plan and perform an individual internal audit is a key knowledge requirement. Whether a member of the internal audit staff, a more senior in-charge auditor, or any member of the internal audit management team, the professional should have a sufficient understanding to assess risks and plan the internal audit, to visit the audit site and start the engagement, to prepare workpapers documenting those audit activities, and to summarize results in preparation for the concluding internal audit report.

Because so many different types of internal audits are performed, we have not tried to outline the steps necessary to perform one generic internal audit. However, an internal auditor should have a good understanding of the *International Standards for the Professional Practice of Internal Auditing,* as summarized in Chapter 8, as well as many of the internal audit planning and performance tools. The standards are a key, however. They outline the steps that an internal auditor *must* follow.

EXHIBIT 7.11 Internal Audit Process: Summarized Steps

The internal audit process through the conclusion of fieldwork:

1. As part of audit planning, perform risk analysis to identify potential control risks.
2. Based on results of the risk analysis and other constraints, develop audit plan.
3. Preliminarily schedule internal audit and allocate resources.
4. Review any past audit reports and workpapers covering audit area.
5. Visit site and perform field survey covering area of planned audit.
6. Based on established workpapers and field survey, prepare audit programs.
7. Prepare and deliver engagement letter for audit, and plan to start internal audit.
8. Begin internal audit fieldwork and planned internal audit.
9. Document processes and perform planned audit procedures.
10. Develop audit point sheets covering preliminary internal audit findings.
11. Complete audit documentation and summarize potential audit findings.
12. Complete internal audit fieldwork and review proposed findings with auditee.

The most important values that the internal audit process provides to the audit committee and management are the reported results of the detailed audits performed in the field or as part of overall operations. Gathering initial evidence, performing the audit, and reporting initial findings to management are all part of this internal audit process. Exhibit 7.11 summarizes these steps for performing internal audits up through the completion of the fieldwork. Once the fieldwork has been completed, the next step is the preparation of the actual audit report, as discussed in Chapter 17.

CHAPTER 8

Standards for the Professional Practice of Internal Auditing

Every profession requires a set of standards to govern its practices, general procedures, and ethics. These standards allow specialists performing similar work to call themselves professionals because they are following a recognized and consistent set of best practices standards. The key standards for internal auditors are the Institute of Internal Auditors (IIA's) *International Professional Standards for the Practice of Internal Auditing* (IIA standards), a set of guidance materials that in the pre-Web paper-document days were known to many internal auditors as the *Red Book*. These standards have gone through multiple revisions over the years. Changes to these standards over time reflect the way the profession of internal auditing is changing. For example, the IIA released a major change to its standards in 2004 with guidance for normal internal audit attest functions and for an internal auditor acting as an internal enterprise consultant. This clarification of internal audit's consulting role was needed and is discussed in Chapter 28.

The year 2009 brought some significant new changes to internal audit standards. Standards that in the past were more guidance directed; using phrases like "an internal auditor should . . ." are now far more mandatory and specify practice areas where an internal auditor "must" follow this standards guidance. This chapter summarizes the current IIA standards and provides guidance on how internal auditors should apply them. An understanding of the IIA's *International Standards for the Professional Practice of Internal Auditing* is an absolute internal auditor common body of knowledge (CBOK) *must* requirement for all internal auditors. These standards provide the support for many if not all internal audit professional activities.

This chapter also revisits the IIA code of ethics for internal auditors, an important supporting foundation for internal auditors in today's world of frequent open questions regarding professional ethics. We also consider the code of ethics for the Information Systems Audit and Control Association (ISACA) professional organization. ISACA members are often IIA or certified public accountant members as well and many are information technology (IT) audit specialists, but their code of ethics places a special emphasis on their IT-related activities. Although ISACA does not have the same type of standards as the IIA, its CobiT (*C*ontrol *ob*jectives for *i*nformation and related *T*echnology) IT internal control framework and information regarding their related professional group, the IT Governance Institute, are discussed in Chapter 5. Chapter 31 introduces another very important set of internal audit standards, the quality audit guidance and standards from the American Society

for Quality (ASQ). ASQ's internal audit standards and its quality auditors represent a different dimension and discipline from the IIA's approaches and standards. They also represent an area that must be better represented and understood in the overall world of internal auditing.

The IIA's *International Standards for the Professional Practice of Internal Auditing* represent a must-know set of requirements for internal auditors today. The sixth edition of this volume contained extensive extracts from the older IIA standards; this chapter introduces the current, recently released standards. While any standards are an evolving set of rules that may not exactly reflect all industry practices at a point in time, they recognize a set of guidelines for internal auditors worldwide to follow in their service to management. The new IIA standards, summarized in this chapter, are available from the IIA.[1] They represent important guidance for today's internal auditor and must be in every internal auditor's professional library.

8.1 Internal Auditing Professional Practice Standards

Internal auditors work in a large variety of enterprises and are asked to perform audit reviews in a diverse number of operational and financial areas. Despite this diversity, audit committees and senior management expect their internal auditors to perform reviews in a competent and consistent manner. Internal audits performed using a set of recognized standards are a key approach to meet those management expectations. As the premier and leading worldwide internal audit professional enterprise, the IIA, through its Internal Auditing Standards Board, develops and issues standards that define the basic practice of internal auditing. The IIA standards are designed to:

- Delineate basic principles for the practice of internal auditing
- Provide a framework for performing and promoting a broad range of value-added internal audit activities
- Establish the basis for the measurement of internal audit performance
- Foster improved organizational processes and operations

The standards aid in this process; they provide a guideline for both the audit committee and management to measure their internal auditors as well as for internal auditors to measure themselves. The standards also set some constraints upon internal audit activity.

(a) Background of the IIA Standards

Chapter 1 talked about the early background of internal auditing, a profession that really developed its own standards and processes. Its professional organization, the Institute of Internal Auditors, first issued what was called the *Standards for the Professional Practice of Internal Auditing* in 1978 with an objective "to serve the entire profession in all types of business, in various levels of government, and in all other enterprises where internal auditors are found . . . to represent the practice of internal auditing as it must be." Prior to these 1978 standards, the most authoritative document was called the *Statement of Responsibilities of Internal Audit,* that was originally issued by the IIA in 1947 and subsequently revised over the years until the current standards. The author of this book's first edition, Victor Brink, played a

major role in the development of the first IIA standards. The foreword to the 1978 IIA standards describes them as "the criteria by which the operations of an internal auditing department are evaluated and measured." This foreword goes on to state: "Compliance with the concepts enunciated by the Standards is essential before the responsibilities of the internal auditor can be met."

The standards were developed by the IIA's Professional Standards Committee based on its professional expertise as well as comments received from IIA members and other interested parties. Because of the diverse group of participants who developed these earlier standards, their final language often had some overlap, compromise, and incompleteness. As a result, individual standards and guidelines still may be subject to varying interpretations.

All internal auditors today, as members of the IIA, are expected to follow these standards. It would be a rare internal audit function that did not have an internal audit charter, as was discussed in Chapter 7, and those charters should strongly affirm adherence to the IIA's standards. Internal auditors may have also come from some other professional areas, such as the banking industry or from an external audit firm. Many such disciplines have their own professional standards that generally are not in conflict with the IIA standards. They may use slightly different terminology, as will be discussed with the ISACA code of ethics, but they must follow audit practices that generally fit under the IIA standards. As a matter of practice, however, the IIA's *International Standards for the Professional Practice of Internal Auditing* govern the work of internal audit, and knowledge of these standards is an important CBOK requirement. When there appears to be a conflict and when the individual who questions that conflict is an internal auditor, the IIA's standards take precedence over any conflicting professional standards.

The IIA has historically published these standards in a small publication known as the *Red Book*. With a changing world and impressions of the role of internal auditors, these standards have changed over the years. There was a major update in 2001, and a revised set of standards was issued in 2004. This section discusses the current 2009 standards and some background on the standards as they have developed over the years.

The older IIA standards, up through the year 2004 releases, sometimes contained an almost impossible level of detail. For example, an older general auditing standard on follow-up procedures guidance for completed audits had *23* individual sub- or sub-sub clarifying standards on these follow-up requirements. While the IIA standards have always contained good general guidance, the older standards were often far too specific. For example, the substandard of the older section 440.01.12.a states that the "Director of Internal Audit should establish the procedures for the time frame in which audit report responses are required." While certainly a valid guideline, it does little good to tell an auditee that IIA standards "require" that their audit report responses must be delivered in seven days if their response is that it will take 10 days. This is just one small example. Many of the older IIA standards were almost too detailed for effective internal audit management. Current IIA standards provide a more much realistic set of guidance materials to allow an internal audit function to perform effectively and efficiently. Standards of past years were complex, sometimes difficult to enforce, and often followed only in a general broad manner.

There was a major change to the IIA standards with the 2004 revisions that permitted internal auditors to act as consultants as well as their traditional attest role as auditors. These changes are highlighted in Chapter 28 describing an internal

auditor as an enterprise consultant. Earlier standards, going back to the early days of internal auditing, prohibited internal auditors from acting as consultants. This prohibition was often ignored over the years, but the 2004 revisions clarified this issue. It divided IIA standards into attest guidance covering internal audit assurance activities and others for internal audit consulting work.

This was a major change to IIA internal auditing standards. In particular, it allowed internal auditors to help in the reviews and assessments of internal controls under the Sarbanes-Oxley Act's (SOx) Section 404 internal controls assessment requirements, as discussed in Chapter 4. Further standards changes can be proposed by IIA volunteer professional committees, which receive requests for changes to the standards, develop proposed formats for member comment, and then issue them as a new revision. A small but significant change to the standards was introduced in 2008 in draft form with a new set of IIA standards released in January 2009.

(b) IIA's Current Standards: What Has Changed

IIA standards are updated regularly to reflect current needs by both business and practicing internal audit professionals. For example, in 2007, because of some expressed professional concerns about who is reviewing the internal auditors, the standards were revised to add Attribute Standard 1312 on External Assessments:

> *External assessments should be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization. The potential need for more frequent external assessments as well as the qualifications and independence of the external reviewer or review team, including any potential conflict of interest, should be discussed by the CAE [chief audit executive] with the Board. Such discussions should also consider the size, complexity and industry of the organization in relation to the experience of the reviewer or review team.*

This was a significant change to internal auditing standards. Discussed in Chapter 31, the new standard calls for a qualified external reviewer to visit an internal audit function to assess its quality procedures and standards. The IIA publishes what are called practice advisories on all of its standards, including this change. For external reviews, two practice advisories outline detailed requirements for these reviewers, including that an external review team should consist of individuals who are competent in the professional practice of internal auditing and the external assessment process. The advisories cover all aspects of this significant change to internal audit practices.

The 2007 IIA standards requirement for independent quality assurance reviews was a major change to internal audit practices. At the time this book goes to press, it has not been actively embraced by all internal audit functions. The once-every-five-year requirement does not have strong beginning and end date requirements nor does it have any provision allowances for the size of the enterprise. For example, when the SOx section 404 requirements were first released for public corporations, compliance dates were staggered by the size of the enterprise and whether it was domestic or foreign. However, the IIA has established peer review processes, where other internal auditors have volunteered to conduct these independent quality assurance reviews, and an increasing number of consulting firms are offering these

services. All internal auditors should be aware of the quality review requirements, and CAEs must inform their audit committees of this requirement and make arrangements for such periodic reviews.

(c) 2009 New Internal Audit Standards

In January 2008, the IIA released a draft version of revised IIA standards. These draft changes have gone through an exposure draft period and were released in January 2009. The changes are significant in that they revise all of the standards requirements from words stating that an internal auditor *should* to that an internal *must.* For example and with the change emphasized in bold italics, the older Standard 1100 on internal auditor independence and objectivity stated, "The internal audit activity ***should*** be independent, and internal auditors ***should*** be objective in performing their work." Only a one-word change but a very important one, the new revisions state, "The internal audit activity ***must*** be independent, and internal auditors *must* be objective in performing their work." The proposed change is significant when a CAE is asked by the audit committee if they are compliant with internal auditing standards. As this book goes to press, these new standards have just been officially released. This change in IIA standards requirements from *should* to *must* may be one of the most significant changes in the practice of internal auditing since its founding by Victor Brink. Although some might argue that should and must mean about the same thing, there are expected compliance requirements for internal auditors.

The next sections describe all of the IIA standards, based on the just-released 2009 version. There can always be changes, and internal auditors should always consult the IIA Web site (www.theiia.org) for the current official version of these standards. These standards set the rules for all internal audit activity, whether performing internal audits, serving as an internal consultant, or managing the overall internal audit function.

8.2 Content of the IIA Standards

The current version of the standards consists of what are called attribute standards, performance standards, and implementation standards. The attribute standards address the characteristics of enterprises and parties performing internal audit activities. The performance standards describe the nature of internal audit activities and provide quality criteria against which the performance of these services can be evaluated. While the attribute and performance standards apply to all internal audit services, the implementation standards also apply to specific types of engagements and are further divided between standards for assurance and consulting activities. This split reflects the fact that internal auditors sometimes do strictly audit assurance–type projects, such as reviewing internal control effectiveness in some areas, and do work related to internal audit consulting. Many of the other chapters in this book cover internal audit assurance or attest activities; Chapter 28 focuses on internal auditors as enterprise consultants.

The attribute standards are numbered in sections as part of the number 1000 series of standards, while performance standards are classified in the 2000 series. Implementation standards, further designated as (A) for assurance or (C) for consulting, are organized under each of these attribute and performance standards. The

next sections describe the attribute and performance standards in some detail as well as some of the descriptive implementation standards. Recognizing that internal auditors may be asked just to review internal controls or to act more as internal consultants, there may be multiple sets of implementation standards: a set for each of the major types of internal audit activity.

Our objective here is not, however, just to reproduce these new IIA published standards but to describe their content and how they have changed or are evolving over recent years. All internal auditors should obtain a copy of these standards from the IIA and develop a good understanding of them. Knowledge of the standards is a CBOK requirement for all internal auditors, and the IIA Web site is an official source for these internal audit standards.

(a) Internal Audit Attribute Standards

Attribute standards address the activities of enterprises and individuals performing internal audit activities. Numbered from paragraph number 1000 to 13000, they cover broad areas that define the attributes of today's modern internal auditor. Here, as well as with the performance standards to be discussed, we have listed and summarized these standards (listed by their standards paragraph numbers):

1000—Purpose, Authority, and Responsibility. The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the standards, and approved by the board of directors. Separate implementation standards here state that internal auditing assurance and consulting services must be defined in the internal audit charter.

1100—Independence and Objectivity. The internal audit activity must be independent, and internal auditors must be objective in performing their work. Subsections under this discuss the importance of both individual and organizational objectivity as well as the need to disclose any impairment to internal audit independence or objectivity.

1110—Organizational Independence. While the IIA standards do not specify that internal audit should report to the audit committee, that reporting relationship must be free from any interference in determining the scope of internal auditing, performing work, and communicating results. While we often think of internal audit as a key component in today's SOx-defined corporate world with board audit committees, internal audit can operate in many different international locations or for many different types of enterprises. Whether serving a not-for-profit organization in the United States or a governmental agency in a developing country, internal audit always must exhibit organizational independence.

1120—Individual Objectivity. This really repeats a basic principle of internal auditing: Internal auditors must have an impartial, unbiased attitude and avoid conflicts of interest.

1130—Impairments to Independence or Objectivity. If internal audit's independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed as part of the audit work. The impairment could be management imposed or one due to the background or other circumstances surrounding an individual internal auditor.

There are several assurance and consulting attribute standards here, but one summarizes this standard:

> **1130.A1 & 2—**Internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an internal auditor provides services for an activity for which the internal auditor had responsibility within the previous year.
>
> **1130.C1 & 2—**Internal auditors may provide consulting services relating to operations for which they had previous responsibilities. If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure must be made to the client prior to accepting the engagement.

This is an important standard. Because of their specialized knowledge, internal auditors sometimes are asked to go back to a group that they once audited. No matter how hard they may try to act to the contrary, others often may not view them as objective.

1200—Proficienc and Due Professional Care. Engagements must be performed with proficiency and due professional care. There is an important proposed new implementation standard here:

> **1210.A1—** The CAE must obtain competent advice and assistance if the internal audit staff lacks the knowledge, skills, or other competencies needed to perform all or part of the engagement.
>
> **1210.A2—** An internal auditor must have sufficient knowledge to identify the indicators of fraud and the manner in which it is managed by the organization but is not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

As discussed in Chapter 25, this guidance is somewhat weak. The American Institute of Certified Public Accountants under Statement on Auditing Standards (SAS) No. 99 requires external auditors to think aggressively about "red flags," indicators that might point to the possibility of fraud, as well as to look for potential fraud in the course of their audits. Although this is certainly an IIA professional standards decision, we feel that internal auditors should maintain a greater awareness about the possibility of fraud in the course of their internal audits. Internal auditors are often the best investigators to find these potential fraud situations. For example, an external auditor may have little contact with a remote sales office, but internal audit may visit that same office as part of a regularly scheduled internal audit and observe its operations.

> **1210.A3—** Internal auditors must have sufficient knowledge of key information technology risks and controls available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

Recognizing that there is a need for IT audit specialists, the standard states that *all* internal auditors *must* have an understanding of IT risks and controls. However,

although the draft version of the standards stated that internal auditors must consider the use of "technology-based audit" tools and techniques, that requirement has now been dropped. Computer-assisted audit techniques, discussed in Chapter 21, are part of the tool kits of many internal auditors.[2]

1220—Due Professional Care. Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility. Another section of these standards goes on to state that in exercising due professional care, an internal audit must consider:

- Extent of work needed to achieve the engagement's objectives.
- Relative complexity, materiality, or significance of matters to which assurance procedures are applied.
- Adequacy and effectiveness of risk management, control, and governance processes.
- Probability of significant errors, irregularities, or noncompliance.
- Cost of assurance in relation to potential benefits.

This internal audit standard really says that an internal auditor must be cautious in beginning and performing an internal audit. The first of these bullet points, the extent of work, says that an internal auditor, for example, must perform an adequate level of investigation and testing before just coming to a final audit recommendation.

1220.A2 —In exercising due professional care the internal auditor must consider the use of technology based audit and other data analysis techniques.

1220.A3— The internal auditor must be alert to the significant risks that might affect objectives, operations, or resources. However, assurance procedures alone, even when performed with due professional care, do not guarantee that all significant risks will be identified. As discussed in Chapter 6, an understanding of risk assessment techniques is an increasingly important CBOK area for internal auditors. This guidance has been part of the IIA standards going back to its early versions and must be part of an internal auditor's procedures.

The standards continue in this section with 1230—Continuing Professional Development, a standard on the requirement for continuing professional education and development.

1300—Quality Assurance and Improvement Program. The CAE must develop and maintain a quality assurance and improvement program that covers all aspects of internal audit activity and continuously monitors its effectiveness. The quality assurance and improvement program must be designed to enable an evaluation of the internal audit activity's conformance with internal auditing standards as well as an evaluation of whether internal auditors apply the code of ethics. The program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for improvement.

The IIA standards here call for both internal and external quality reviews and emphasize the importance of good quality assurance processes within internal audit. Quality assurance as well as quality audits are discussed in Chapter 31. Two important standards here are:

1311—Internal Assessments. Internal audit management must have an internal assessment process in place that includes both the ongoing monitoring of the performance of the internal audit activity and periodic reviews performed through self-assessment or by other persons within the enterprise with sufficient knowledge of internal audit practices.

1312—External Assessments. As discussed previously, external assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization. The CAE must discuss this need for more frequent external assessments with the board audit committee and the qualifications and independence of the external reviewer or review team, including any potential conflicts of interest.

This section of the standards requires that the CAE may state the internal audit activity conforms with the IIA standards only if the results of the quality assurance and improvement program support this statement. In addition, when internal audit it not in compliance with the code of ethics or the IIA standards, the CAE must disclose the nonconformance and its impact to senior management and the board.

(b) Internal Audit Performance Standards

Performance standards describe the nature of internal audit activities and provide quality criteria against which these services can be measured. There are six performance standards, outlined next, along with substandards and implementation standards that apply to compliance audits, fraud investigations, or control self-assessment projects. We are summarizing the standard here for the purpose of describing internal audit processes; the interested professional must contact the IIA to obtain the standards in either computer-downloaded or printed format.

2000—Managing the Internal Audit Activity . The CAE must effectively manage the internal audit activity to ensure it adds value to the enterprise. This standard covers six substandards, 2010 to 2060.

2010—Planning. The CAE must establish risk-based plans consistent with the enterprise's risk management framework to determine the priorities of the internal audit's activities. If an enterprise-level risk management framework does not exist, the CAE should use his or her own judgment of risks after consultation with senior management and the board.

2020—Communication and Approval. The CAE must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. This communication must also include the impact of resource limitations.

2030—Resource Management. The CAE must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

2040—Policies and Procedures. The CAE must establish policies and procedures to guide the internal audit activities that are appropriate to the size and structure of internal audit activities and the complexity of its work.

2050—Coordination. The CAE should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

2060—Reporting to Senior Management and the Board. The CAE must report periodically to senior management and the board on internal audit's performance relative to its plan. Reporting must include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.

2100—Nature of Work . In strong words, the IIA standards state that internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach. Earlier IIA standards did not really address the important areas of governance and risk management.

2110—Governance. Internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of these objectives:

- Promoting appropriate ethics and values within the enterprise
- Ensuring effective organizational performance management and accountability
- Communicating risk and control information to appropriate areas of the organization
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management

In addition, internal audit must evaluate the design, implementation, and effectiveness of the enterprise's ethics-related objectives, programs, and activities. Also, internal audit must assess whether IT governance processes sustain and support the enterprise's strategies and objectives.

2120—Risk Management. Internal audit must assist the enterprise by identifying and evaluating significant exposures to risk and contributing to the improvement of risk management and control systems. Determining whether risk management processes are effective is a judgment resulting from an internal auditor's assessment that:

- Organizational objectives support and align with an enterprise's mission
- Significant risks are identified and assessed
- Appropriate risk responses are selected that align risks with the enterprise's risk appetite
- Relevant risk information, enabling staff, management, and the board to carry out their responsibilities, is captured and timely communicated across the enterprise

Risk management processes should be monitored through ongoing management activities, separate evaluations, or both to monitor and evaluate the effectiveness of the enterprise's risk management system. Internal audit activity must evaluate risk

exposures relating to the enterprise's governance, operations, and IT regarding the Committee of Sponsoring Organizations' standards of internal control.

2200—Engagement Planning. Internal auditors must develop and record a plan for each engagement, including the scope, objectives, timing, and resource allocations**.** An important aspect of all internal audits, planning is discussed in Chapter 7.

2201—Planning Considerations. In planning an audit engagement, internal auditors must consider:

- The objectives of the activity being reviewed and the means by which the activity controls its performance
- The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level
- The adequacy and effectiveness of the activity's risk management and internal control processes compared to a relevant control framework or model
- The opportunities for making significant improvements to the activity's risk management and control processes

2210—Objectives Must Be Established for Each Engagement. Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review, and engagement objectives must reflect the results of this assessment. The internal auditor must consider the probability of significant errors, irregularities, noncompliance, and other exposures when developing the engagement objectives. This relates to the risk assessment considerations discussed previously. Adequate criteria are needed to evaluate controls. Internal auditors must ascertain the extent to which management has established adequate criteria to determine whether objectives and goals have been accomplished. If the criteria are adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must work with management to develop appropriate evaluation criteria. Consulting engagement objectives must address risks, controls, and governance processes to the extent agreed on with the client.

2220—Engagement Scope. The established scope must be sufficient to satisfy the objectives of the engagement and must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties. If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities, and other expectations must be reached and the results of the consulting engagement communicated in accordance with these consulting standards. This says that an internal auditor can begin an audit as a strictly assurance-level of review but may expand it to a consulting-level audit if there is a need or management request. When performing consulting engagements, internal auditors must ensure that the scope of the engagement is sufficient to address the agreed-on objectives. If internal auditors develop reservations about the scope during the engagement, these reservations must be discussed with the auditee to determine whether to continue with the engagement.

2230—Engagement Resource Allocation. Internal auditors must determine the appropriate resources necessary to achieve the audit engagement

objectives. Staffing must be based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.

2240—Engagement Work Program. Internal auditors must develop and document work programs that achieve the engagement objectives. These work programs must establish procedures for identifying, analyzing, evaluating, and recording information during the engagement. They must be approved prior to their implementation, and any adjustments must be approved promptly. Work programs for consulting engagements may vary in form and content depending on the nature of the engagement.

2300—Performing the Engagement. Internal auditors must identify, analyze, evaluate, and record sufficient information to achieve an audit engagement's objectives and must base conclusions and engagement results on appropriate analyses and evaluations.

2310—Identifying Information. Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives. "Sufficient" information, as defined in these standards, is factual, adequate, and convincing so that a prudent, informed person would reach the same conclusions as the internal auditor. "Reliable" information is the best attainable information through the use of appropriate engagement techniques. "Relevant" information supports engagement observations and recommendations and is consistent with the objectives for the engagement. "Useful" information helps an enterprise meet its goals.

2320—Analysis and Evaluation. Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.

2330—Documenting Information. The CAE must control access to engagement records and must obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate. The CAE also must develop retention requirements for engagement records, regardless of the medium in which each record is stored. These retention requirements must be consistent with the organization's guidelines and any pertinent regulatory or other requirements. When internal audit is acting as a consultant, the CAE must develop policies governing the custody and retention of consulting engagement records, as well as their release to internal and external parties. These policies must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.

2340—Engagement Supervision. Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed. The extent of supervision required will depend on the proficiency and experience of internal auditors and the complexity of the engagement. The CAE has overall responsibility for supervising the engagement, whether performed by or for the internal audit function, but may designate appropriately experienced members of the internal audit function to perform the review. Appropriate evidence of this supervision is documented and retained.

2400 and 2410—Communicating Results. Internal auditors must communicate their engagement results describing the audit's objectives and scope as well as applicable conclusions, recommendations, action plans, and the internal auditor's overall opinion and or conclusions. The final communication of engagement results must, where appropriate, contain the internal auditor's overall opinion and/or conclusions. Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.

When releasing engagement results to parties outside the enterprise, these communications must include limitations on distribution and use of the results.

2420—Quality of Communications. Communications must be accurate, objective, clear, concise, constructive, complete, and timely.

2421—Errors and Omissions. If a final communication contains a significant error or omission, the CAE must communicate corrected information to all parties who received the original communication.

2430—Use of "Conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*." Internal auditors are encouraged to report that their engagements are "conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*." However, internal auditors may use the statement only if the results of the quality assurance and improvement program demonstrate that the internal audit activity conforms to the standards.

2431—Engagement Disclosure of Noncompliance with IIA Standards. When noncompliance with the standards impacts a specific engagement, communication of the results must disclose the:

- Principle or rule of conduct of the code of ethics or standard(s) with which full conformance was not achieved
- Reason(s) for noncompliance
- Impact of noncompliance on the engagement

2440—Disseminating Results. The CAE is responsible for communicating the final audit results to parties who can ensure that the results are given due consideration. If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside the enterprise, the CAE must:

- Assess the potential risk to the organization
- Consult with senior management and/or legal counsel as appropriate
- Control dissemination by restricting the use of the results

In addition, the CAE is responsible for communicating the final results of consulting engagements to clients. During consulting engagements, governance, risk management, and control issues may be identified. Whenever these issues are significant to the organization, they must be communicated to senior management and the board.

2500—Monitoring Progress. The CAE must establish and maintain a system to monitor the disposition of results communicated to management as well as a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.

2600—Resolution of Management's Acceptance of Risks. When the CAE believes that senior management has accepted a level of residual risk that *may be* unacceptable to the enterprise, the CAE must discuss the matter with senior management. If the decision regarding residual risk is not resolved, the CAE and senior management must report the matter to the board for resolution.

The current IIA standards represent a significant improvement over the older and very lengthy standards that were in place through the 1990s. The standards conclude with a glossary of terms to better define the roles and responsibilities of

internal auditors. Various glossary terms are introduced in subsequent chapters but one that is important for internal auditors is the definition of *independence*. The word frequently appears in internal auditing literature, but the official definition of internal auditor independence is:

> *Independence is the freedom from significant conflicts of interest that threaten objectivity. Such threats to objectivity must be managed at the individual auditor level, the engagement level, and the organizational level.*

This is an important concept today. We again emphasize that preceding paragraphs are *not the verbatim IIA standards* but an edited and annotated version. They are also based on the just-released current version of the standards. The chapter does not include some of the more minor standards statements; in some cases a few words have been changed, and descriptive comments have been added. As stated, internal auditors are advised to obtain the official version of these standards through the Institute of Internal Auditors at www.theiia.org.

The one-word change—to "the auditor *must*" from "the auditor *should*"—represents a major change to internal auditor professional standards. Internal audit functions can no longer elect to review portions of these standards just as good guidance and then not really follow them. While the term *must* leaves a little flexibility if the CAE can justify some very strong reason not to follow some standards requirement, internal audit almost always should be expected to follow the guidance of the IIA standards. A strong understanding of these standards and the requirement to follow them is a CBOK requirement for all internal auditors.

8.3 Codes of Ethics: The IIA and ISACA

The purpose of the IIA's code of ethics is to promote an ethical culture for the profession of internal auditing. This code of ethics is displayed in Exhibit 8.1. The code supports the trust placed on users of internal audit services for their objective assurances about risk management, internal control, and governance. The IIA's current code was released in 2000 and is based on the principles of internal auditor integrity, objectivity, confidentiality, and competency.[3] These are the behavioral norms expected of internal auditors and are intended to guide their ethical conduct.

The IIA code of ethics replaces an earlier 1988 version that had 11 specific articles defining preferred practices; that version, in turn, replaced a 1968 version. The current 2000 version, with its emphasis on integrity, objectivity, confidentiality, and competency, is much easier to understand and recognize than the rather detailed articles in prior versions. As a minor note, the 1988 version used the term *Members and CIAs* in each of its articles. The current code simply says *Internal Auditors*, perhaps a better terminology. Any person performing internal audit services, whether a member of the IIA or not, should follow this code of ethics. Professional certificates, including the Certified Internal Auditor (CIA) designation, are discussed in Chapter 27.

This IIA code of ethics applies to both individuals and entities that provide internal auditing services. For IIA members and recipients of or candidates for IIA professional certifications, breaches of the code will be evaluated and administered according to IIA Bylaws and Administrative Guidelines. The IIA goes on to state that

EXHIBIT 8.1 Institute of Internal Auditors Code of Ethics

The Institute of Internal Auditors
Code of Ethics

1. Integrity
Internal auditors:
1.1. Shall perform their work with honesty, diligence, and responsibility.
1.2. Shall observe the law and make disclosures expected by the law and the profession.
1.3. Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession of internal auditing or to the organization.
1.4. Shall respect and contribute to the legitimate and ethical objectives of the organization.

2. Objectivity
Internal auditors:
2.1. Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment. This participation includes those activities or relationships that may be in conflict with the interests of the organization.
2.2 Shall not accept anything that may impair or be presumed to impair their professional judgment.
2.3 Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.

3. Confidentialit
Internal auditors:
3.1 Shall be prudent in the use and protection of information acquired in the course of their duties.
3.2 Shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization.

4. Competency
Internal auditors:
4.1. Shall engage only in those services for which they have the necessary knowledge, skills, and experience.
4.2 Shall perform internal auditing services in accordance with the *Standards for the Professional Practice of Internal Auditing*.
4.3 Shall continually improve their proficiency and the effectiveness and quality of their services.

Source: Adopted by The IIA Board of Directors, June 17, 2000. Copyright © 2000 by The Institute of Internal Auditors, 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201. Reprinted with permission.

even if a particular conduct is not mentioned in this code, this does not prevent the conduct or practice from being unacceptable or discreditable. Violators of this code, whether an IIA member, certification holder, or candidate, can be held liable for disciplinary action.

ISACA, as well as its affiliated research arm, the IT Governance Institute, is the professional audit enterprise that represents or speaks primarily for IT auditors. ISACA was originally known as the EDP Auditor's Association, a professional group founded in 1969 by a group of internal auditors who felt the IIA was not giving sufficient attention to computer systems and their related technology-related internal controls. We have almost forgotten that EDP stands for electronic data processing, an almost archaic term, and we now have ISACA. It is still leading the IIA on technology-related issues. ISACA is also the professional enterprise that administers the CISA (Certified Information Systems Auditor) examination and program and is responsible for the CobiT internal control framework discussed in Chapter 5.

EXHIBIT 8.2 ISACA Code of Professional Ethics

The Information Systems Audit and Control Association, Inc. (ISACA) sets forth this Code of Professional Ethics to guide the professional and personal conduct of members of the association and/or its certification holders.

Members and ISACA certification holders shall:

1. Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards and best practices.
3. Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.
4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities, which they can reasonably expect to complete with professional competence.
6. Inform appropriate parties of the results of work performed; revealing all significant facts known to them.
7. Support the professional education of stakeholders in enhancing their understanding of information systems security and control.

Failure to comply with this Code of Professional Ethics can result in an investigation into a member's, and/or certification holder's conduct and, ultimately, in disciplinary measures.

With its IT audit and governance orientation, ISACA represents a somewhat different group of auditors. Historically, ISACA drew a large number of members from IT audit specialists and public accounting external audit firms, and it has had a very strong international membership. Many IIA members are also ISACA members. While the two groups do not have many joint meetings or other endeavors, each represents an important segment of the internal audit community.

While ISACA—fortuitously—does not have its own set of professional standards, it does have a code of ethics as shown in Exhibit 8.2. Because of its IT heritage, the ISACA code is more oriented to technology issues. It is a set of professional standards that applies to and should be of particular value to IT audit professionals. Although the wording is different, there is nothing in the ISACA code that is really contrary to the IIA code. Internal auditors, whether working primarily in IT areas or with a more general internal controls orientation, should exercise strong ethical practice in their work.

Notes

1. Institute of Internal Auditors, *International Standards for the Professional Practice of Internal Auditing* (Altamonte Springs, FL: 2009).
2. See Robert R. Moeller, *Computer Audit, Control, and Security* (New York: John Wiley & Sons, 1989). The current edition is out of print, but a new edition is in preparation.
3. www.theiia.org/guidance/standards-and-practices/professional-practices-framework/code-of-ethics/code-of-ethics.

CHAPTER 9

Testing, Assessing, and Evaluating Audit Evidence

The internal audit process begins with establishing audit objectives, then planning and performing the internal audit, and finally evaluating the audited results to determine if the audit objectives have been satisfied, if supporting internal controls are adequate, if the materials reviewed are sufficient to develop an audit conclusion, and if there is a need for corrective-action-based audit recommendations. This process of testing, assessing, and then evaluating audit evidence can be a challenge for many internal auditors. For example, an internal auditor can review a sample of 100 items and find no problems with 99 of them. Should that one internal control problem exception cause the internal auditor to highlight that one exception as an overall internal control problem, or should the internal auditor give that single exception a "pass" and go forward? There often are no easy answers, but an experienced internal auditor should be should be able to evaluate this audit evidence and make the appropriate decision.

While Chapter 7 outlined steps for performing an internal audit and Chapter 8 described the Institute of Internal Auditors (IIA) professional standards necessary for performing internal audits, this chapter reviews the processes of testing and evaluating audit evidence. These are the common body of knowledge (CBOK) steps necessary to look at audit evidence and then to develop appropriate audit conclusions and recommendations based on that evidence. This is the key step in the overall internal audit process.

9.1 Gathering Appropriate Audit Evidence

Internal auditors make assessments about audit issues or satisfy their audit objectives through detailed reviews of what is called *audit evidence.* That is, an internal auditor generally does not look at every item in an area of audit concern to develop evidence to support an audit. Rather, the internal auditor examines a limited set of files or reports and reviews selected sample items to develop audit conclusions over the entire set or population of data. A review of equipment contracts for a smaller manufacturer may not involve more than a very limited number of items where the auditor can perform a 100% review of the audit evidence, the equipment contract records. This approach is much more difficult when internal audit is faced with a large population of items to examine—hundreds, thousands, or even more.

In the early days of internal auditing, 100% examinations of transactions or documents were common to assess control procedures compliance. As enterprises and their processes grew larger and more complex, this 100% examination approach was often not feasible, so internal auditors typically selected a sample to develop an audit conclusion. In addition, they needed some way to review these large masses of computerized data. There is a major internal audit challenge here. An internal auditor needs a consistent approach to sample a portion of items from a large population of data and then to draw audit conclusions based on that limited sample.

The internal audit sampling challenge is to extract a sample of items that will be representative of the entire population. If there are 100,000 transactions and if an internal auditor looks at only 50 of them, finding 10 exceptions (20% of the sample), can the auditor conclude that 20% of the entire population of transactions, or 20,000, are exceptions? This audit conclusion is true only if the sample of 50 drawn is representative of the entire population. Audit sampling techniques can help an internal auditor determine an appropriate sample size and develop an opinion for this type of audit task.

Audit sampling has two major branches: statistical and nonstatistical. Statistical sampling is a mathematical-based method of selecting representative items that reflect the characteristics of the entire population. Using the results of audit tests on the statistically sampled items, an internal auditor can then express an opinion on the entire group. For example, an auditor could develop a statistical sample of items in an inventory, test items from that sample for their physical quantity or value, and then express an opinion on the value or accuracy of the entire inventory. Nonstatistical sampling, also called judgmental sampling, is not supported by mathematical theory and does not allow an internal auditor to express *statistically precise* opinions on the entire population. Nevertheless, nonstatistical or judgmental sampling is often a useful audit tool.

9.2 Audit Assessment and Evaluation Techniques

When planning any audit that includes the examination of a large number of transactions or other evidence, an internal auditor should always ask the question: Should I use audit sampling? The correct answer here is often not just a simple yes or no but may be complicated by such factors as the number or nature of items to be sampled, a lack of technical expertise or computer software availability to do the sampling, a fear of the mathematical focus of sampling, and the potential nonacceptance of the sampling results by management. *Sampling* also is a term that is frequently misused by internal auditors. All too often, when faced with a file cabinet filled with hundreds of documents to review, the auditor pulls out one or two items from the front and performs audit procedures based on this limited selection. While this examination of two items may be appropriate for an audit observation, an internal auditor *should not* try to draw conclusions for the entire population based on that limited sample. To develop an audit conclusion over these data, internal auditors need a process where they should:

- Understand the total population of items of concern and develop a formal sampling plan regarding the population of items.
- Draw a sample from the population based on that sample selection plan.

- Evaluate the sampled items against audit objectives.
- Develop conclusions for the entire population based on audit sample results.

These steps represent the process of audit sampling, the process of examining less than 100% of the items within an account balance or class of transactions for the purpose of drawing some form of conclusion for the entire population based on the sample audit results. Audit sampling can be a very attractive and effective option for internal auditors, and basic audit sampling skills should be an internal audit CBOK requirement.

Why use audit sampling? While we often hear reports on the results of statistical sampling techniques in consumer research, government studies, or quality-control testing on a production assembly line, audit sampling can be a very effective tool for internal auditors as well. While 100% examinations work for limited amounts of audit evidence, internal audit almost always must review a sample—either very large or small—of the audit evidence. The internal auditor would then draw an audit conclusion based on the results of that sample. With formal audit sampling, internal audit can draw a conclusion along the lines of "Based on the results of our audit sample, we are 98% certain the true inventory balance is between X and Y." This type of statement and process are discussed in greater detail in the paragraphs that follow.

Formal audit sampling is a powerful tool, and with some education and practice, internal auditors can begin to use it easily and effectively. Whenever an internal auditor needs to draw conclusions based on a population of multiple items but does not want to examine the entire population, audit sampling can introduce better and more efficient audits. Reasons that encourage the use of audit sampling and statistical sampling in particular include:

- **Conclusions may be drawn regarding an entire population of data.** If a statistical sampling method is used, information can be projected accurately over the entire population without performing a 100% check on the population, no matter how large. For example, an internal auditor may be interested in the occurrence of some error condition in a large volume of incoming product freight bills. The auditor could select a statistical sample of these freight bill documents, test the sample for the error condition, and then be able to make a 98% certain type of estimate about the occurrence of that error condition in the entire population of freight bills. This technique typically results in a strong audit position and significant audit savings.
- **Sample results are objective and defensible.** Internal control errors often occur on a random basis over the total items subject to error, and each error condition should have an equal opportunity of selection in an audit sample. An audit test based on random selection is objective and even defensible in a court of law. Conversely, a sample based on auditor judgment could be distorted due to intentional or unintentional bias in the selection process. An auditor looking for potential problems might examine only the larger or sensitive items, ignoring others.
- **Less sampling may be required through the use of audit sampling.** Using mathematics-based statistical techniques, internal auditors often do not need to increase the size of a sample directly in proportion to the size of the population to be sampled. Even though a sample of 60 items may be needed to express an audit opinion over a population of 500 items, that same sample of 60 may still

be sufficient for a population of 5,000. An internal auditor who does not use statistical approaches will often over-sample large populations because of the incorrect belief that larger populations require proportionately larger samples. By using statistics-based sampling procedures, less testing may be required.

- **Statistical sampling may provide for greater accuracy than a 100% test.** When voluminous amounts of data items are counted in their entirety, the risk of significant clerical or audit errors increases. However, a small sample typically receives very close scrutiny and analysis. The more limited sample is subject only to sampling errors resulting from the statistical projection.
- **Audit coverage of multiple locations is often more convenient.** Audits can be performed at multiple locations with small samples taken at individual sites to complete an overall sampling plan. In addition, an audit using comprehensive statistical sampling may be started by one auditor and continued by another. Each of their sample results can be combined to yield one set of audit results.
- **Sampling procedures can be simple to apply.** In years past, an internal auditor often was required to use tables published in sampling manuals or complex computer systems to develop a sampling plan and sample selection. With the availability of laptop computer–based software packages, audit sampling has been simplified. The sampling tools and techniques discussed in this chapter should help to explain the process for internal auditors.

Despite the advantages of audit sampling, an internal auditor must keep in mind that *exact information* cannot be obtained about a population of items based on just a sample, whether it is judgmental or statistical. It is only by making a 100% test and following good audit procedures that an internal auditor can obtain exact information. With nonstatistical, judgmental sampling, information is obtained only about those items examined. With statistical sampling, regardless of the number of items examined, positive information can be obtained about all of the items in the population within a level of statistical confidence. The next sections discuss judgmental and statistical audit sampling—both important internal audit tools. In addition, the discussion on statistical sampling provides guidance on attributes, monetary unit, and variables sampling techniques as well as other techniques for internal auditor use.

9.3 Internal Audit Judgmental Sampling

Although we encourage a more statistical audit sampling approach, nonstatistical judgmental sampling is a very appropriate internal audit procedure in many situations. As its name implies, this approach requires an internal auditor to use his or her best judgment to design and select a sample. No statistical decision rules are used, and the auditor selects only a sampling plan approach that will provide a large enough sample to test the audit objectives, such as whether the internal controls reviewed are operating properly or if the procedures examined are being followed. Judgmental sampling requires an internal auditor to select a representative sample of items in a population of data or transactions for audit review. The sample of the items reviewed will be less than 100% of the entire population but should be sufficient for internal audit to make overall audit conclusions based on those sample

results. For internal auditors, the methods for a judgmental sample selection may take many forms, including:

- **Fixed percentage selection.** An examination of a fixed percentage—such as 10%—of the items or dollars in an audit population. These sample items are often selected haphazardly, with the internal auditor opening a file drawer, for example, and selecting every one or two items or files until the desired sample size is met.
- **Designated attribute selection.** A selection of all or part of the items active during a time period, such as one month in an audit covering a year's transactions. Alternatively, an auditor could select all items having a common characteristic, such as all accounts ending in a particular letter of the alphabet, as part of a review of vendor invoices.
- **Large-value selection.** A selection for audit review of just those items with large monetary or other significant balances.
- **Designated area selection.** An examination of only items readily available, such as those stored in a particular file drawer. Such sample items may be selected because they looked "interesting."
- **Other selected attribute selection.** A review of sensitive items only or items with some other attribute of audit concern. In a review for inactive or obsolete inventory items, an auditor might select for review only those items that appear to be dusty or located in out-of-way locations in the inventory stores area.

Although useful data may be obtained from judgmental samples, the results can be misleading or inaccurate regarding the whole population or account. An internal auditor may look at the accuracy of finance charges for the largest 10% of some account under the assumption that these are the most significant. Even though no significant problems were found for the 10% sampled, the auditor will not know of any significant control problems over the remaining accounts representing the other 90%. Similarly, an internal auditor can select a dusty corner of a warehouse storage space in a search for obsolete inventory. The items found in that area are probably candidates to scrap and be put in an internal audit report comment, but they cannot be assumed to represent the level of obsolescence throughout the entire facility.

When planning a review based on judgmental samples, an internal auditor should make three judgmental sampling decisions.

First, the internal auditor must develop a method of selection and decide what types of items to examine. Internal auditors can be subject to criticism if problems are encountered later that were not included in the sample selection. An examination of all account names starting with the arbitrary first letters *A* and *M* will not reveal a problem for an account with an account name starting with *S.*

The size of the sample is the second audit judgment decision. Auditors sometimes incorrectly select only two or three items located off the top of the deck, review them, and state audit results are based on this very limited and nonrepresentative audit sample. This can be misleading, and managers who receive internal audit report findings often assume that a far larger sample was reviewed. The sample size should be reasonable compared to the entire population. Too small a sample will not represent the overall population, while a too-large sample may be too time-consuming or otherwise expensive to evaluate.

EXHIBIT 9.1 Judgmental Sampling Audit Findings Problems

Example Audit Finding 1: Based on our sample of inventory items, we found three items that were incorrectly labeled. Controls need to be improved to . . .

What Is Wrong Here: There is no reference to the number of items in the inventory, the size of the sample, or the implications of the sample results.

Example Audit Finding 2: Based on our statistical sample of accounts receivable records, we found . . .

What Is Wrong Here: No reference to what is meant by a "statistical sample" and how the internal audit conclusion was developed.

Example Audit Finding 3: We found seven incorrectly valued items in our sample of fixed asset items; based on the results of this sample, we recommend . . .

What Is Wrong Here: There is no explanation of what is meant by the "items in our sample." Reported audit findings should give some details on the size of the population and number of items sampled for the audit.

The third decision is how to interpret and report the audit results from the limited judgmental sample. An internal audit review of excess and obsolete inventory that selects 20 dusty and dirty items from the stores area and finds that 10 are obsolete should not then conclude that 50% of the entire inventory is obsolete based on that sample. The bulk of the stores inventory may be active and appear to be clean. If those active items were not considered in the selection, conclusions from the judgmental sample may be inaccurate. Even though 50% of the dusty and dirty items examined may be obsolete, this does not mean that *the entire* inventory is obsolete. The results from a judgmental sample must be stated very carefully. Exhibit 9.1 provides examples of some ambiguous audit report conclusions based on incomplete judgmental samples. All of these examples point out that the findings were based on some level of judgmental sample. The problem here is that internal auditors frequently refer to their audit sample and draw conclusions from the results even though there has been little statistical support for these sample conclusions. We are showing these as examples of problems in reporting sampling results; Chapter 17 contains a more extensive discussion of reporting internal audit results.

The whole concept behind internal audit judgmental sampling is that item selection is based on the internal auditor's judgment. An internal auditor can select as many or as few sample items that appear appropriate in his or her professional judgment. Often good internal auditors can "smell" a potential problem by looking at an area and selecting a series of items that represent potential problems. However, even though some internal auditors may be right on target when pulling their often arbitrary-size samples, many others may miss significant items or may focus on a few bad apples that do not represent an entire population of otherwise good items. Although there are multiple options of approach here, successful internal auditors often are better off using some form of statistical sampling for audit item selection, as discussed in the next section.

9.4 Statistical Sampling: An Introduction

Statistical sampling is a powerful tool that allows an internal auditor to project the results of an audit sample over the entire population with a strong degree

of accuracy and confidence. Based on the rules of probability, statistical sampling requires the use of established mathematical selection techniques with results that can be projected over the entire population in a manner that will be accepted by the courts, government regulators, and others. Statistical sampling is also one of those topics that many internal auditors took in an undergraduate college course, finishing the class and hoping never to encounter that subject again.

Statistical sampling once was a complex internal audit process requiring a high degree of mathematical and computational skills. Software tools available today eliminate many of these difficulties. We discuss some of the concepts supporting statistical sampling as well as more common approaches to internal audit statistical sampling. Examples are presented to help an internal auditor use statistical sampling more effectively.

(a) Statistical Sampling Concepts

A general understanding of probability and statistical concepts is an important first step for using statistical sampling. This chapter does not attempt to be a statistics textbook, but some basic statistical concepts and terminology are important. While we can draw a statistical sample without the need for an in-depth understanding of statistics interested internal auditors should consult a book on statistical auditing[1] for more information. Some sampling concepts are fairly easy, and a general understanding is important.

We start with some of the important statistical sampling terms. First, the word *population* refers to the total number of items that are subject to an audit, and a *random sample* is the process of selecting a sample where each unit in that population has an equal probability of selection. The random sample 10 should represent the characteristics one of the entire population. However, the characteristics of one random sample drawn by an internal auditor may be different from a sample from the same population drawn by another. To determine how far a sample result differs from that of a 100% test, an internal auditor should have an understanding of the behavior of all possible samples that might be drawn from a population.

Because multiple samples may bring different results, it is important to understand the statistical sampling terms for of measures of central tendency. In audit sampling, the expression *average value* is used to describe the characteristics of a set of sampled data. While internal auditors often work with much larger populations, consider a population of 25 accounts receivable balances with a total value of $86,345.24, as shown in Exhibit 9.2. Statisticians commonly use seven different measures to look at the central tendencies of these data or the degree that the various values are dispersed around a central average. The most common statistical measures for looking at data are the *mean, median, mode, range of data values, variance,* the *standard deviation,* and the *skewness of the data.* Although these central-tendency measures can be calculated today by pressing a function key on a business calculator, an internal auditor should understand their meaning, use, and how they are calculated. We show these values using the Exhibit 9.2 sample data.

- The *mean* is the simple average of the values of items in a population. It is calculated by adding up the total amount in the population of interest—in this example, 25 individual balances for $86,345.24—and then dividing this total by the number of observed items in the population. Although an internal auditor

EXHIBIT 9.2 Sample Population of Accounts Receivable Balances

Item#	A/R Balance	Rank
1	$275.00	3
2	$1,059.25	8
3	$2,564.78	15
4	$9,032.00	22
5	$1,750.00	12
6	$17,110.40	25
7	$1,713.99	11
8	$6,245.32	20
9	$534.89	5
10	$534.89	6
11	$2,564.78	16
12	$1,122.05	9
13	$3,025.88	17
14	$514.99	4
15	$10,554.58	24
16	$1,988.63	13
17	$7,026.50	23
18	$978.00	7
19	$1,654.54	10
20	$3,066.00	18
21	$35.87	1
22	$78.99	2
23	$2,003.00	14
24	$6,995.41	21
25	$3,915.50	19
	$86,345.24	

certainly does not need to worry about it, the Greek μ symbol is often used to report the mean. In this example, the mean or μ is 86,345.24/25 = $3,453.81.

- The *median* is the middle amount value when all of the items in the population are ranked by size. Exhibit 9.2 contains a column labeled "Rank" that shows the ranking of each item by its value or size. Item 21 has been ranked as number 1 because it is the smallest value in the population at $35.87. Item 22 is ranked as number 2 because it is the next smallest. The median is calculated by counting the number of individual items in the population and selecting the one where 50% are larger and the other 50% are smaller. In this example, item 16 has been ranked as number 13 and $1,988.63 is the median for this population. Twelve items are smaller and 12 larger. The median is rarely the same value as the mean. Here the median value is smaller than the mean because there are more items of smaller value in the population.
- The *mode* is the amount or value that occurs most frequently in a population. In this example, two items—numbers 9 and 10—each have a value of $534.89. The mode is generally not a very meaningful measure of statistics. While sometimes it is useful with a larger population with many items bunched around the same general values, a mode is more useful when the data are summarized into a histogram. The histogram for this sample in Exhibit 9.3 shows that the most common value for the sample data is less than $500.

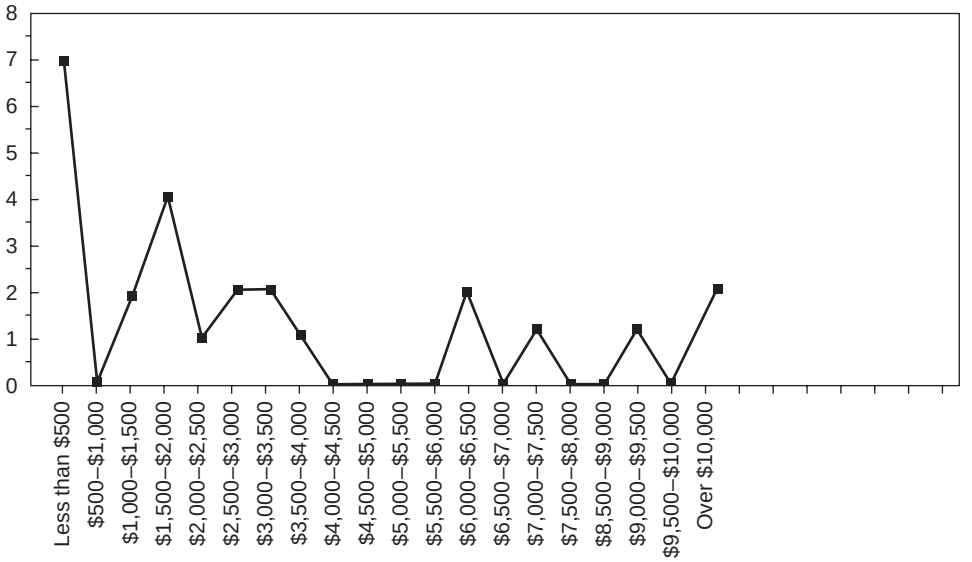


EXHIBIT 9.3 Accounts Receivables Balances Histogram

- The *range* is the difference between the largest and the smallest values in a population. In this example, the range is the difference between item 6 ($17,110.40) and item 21 ($35.87 or $17,074.53). This measure is useful primarily as an indicator of the breadth of the population data. (The range also is discussed as part of measuring dispersion through what is called the standard deviation.)
- The *variance* is a measure of the spread of a distribution, and it is computed as the average squared deviation of each number from its mean. The symbol σ^2, or sigma squared, is a measure of the variance or standard deviation. For example, for a population consisting of the numbers 1, 2, and 3, the mean is 2 and the variance is the square root of this standard deviation calculation:

$$\sigma^2 = \frac{(1-2)^2 + (2-2)^2 + (3-2)^2}{3} = .667$$

- Most professionals should find each of the measures discussed thus far fairly easy to understand, even those who have not had much background in statistics. Many find the concept of *standard deviation* more difficult to understand.

  The standard deviation is a measure of the *variability* of values for individual items in a population. The symbol σ, or sigma, is often used for the standard deviation where:

$$\text{Standard Deviation} = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \bar{x})^2}{\eta}}$$

  Standard deviation tells the auditor how much variation of values exists around the mean or central point. The third column in Exhibit 9.4 shows the $x_i - \overline{X}$ differences, and the fourth column shows differences as squared values

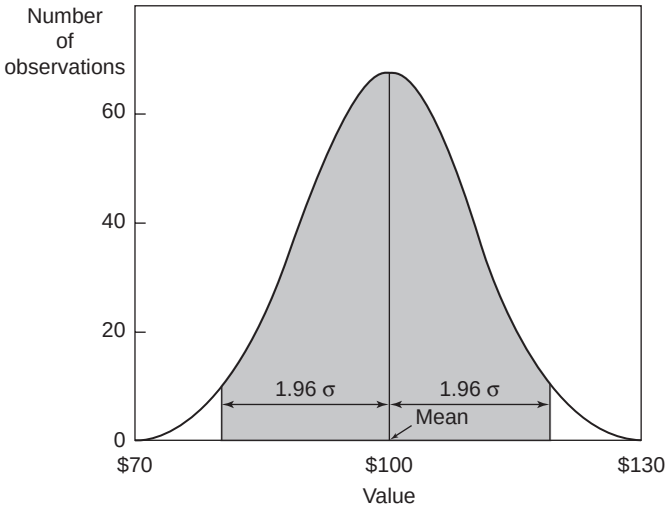
EXHIBIT 9.4 Standard Deviation Example Calculations

n	x_i	$x_i - \overline{X}$	$(x_i - \overline{X})^2$
1	275.00	(3,178.81)	10,104,833.02
2	1,059.25	(2,394.56)	5,733,917.59
3	2,564.78	(889.03)	790,374.34
4	9,032.00	5,578.19	31,116,203.68
5	1,750.00	(1,703.81)	2,902,968.52
6	17,110.40	13,656.59	186,502,450.43
7	1,713.99	(1,739.82)	3,026,973.63
8	6,245.32	2,791.51	7,792,528.08
9	534.89	(2,918.92)	8,520,093.97
10	534.89	(2,918.92)	8,520,093.97
11	2,564.78	(889.03)	790,374.34
12	1,122.05	(2,331.76)	5,437,104.70
13	3,025.88	(427.93)	183,124.08
14	514.99	(2,938.82)	8,636,662.99
15	10,554.58	7,100.77	50,420,934.59
16	1,988.63	(1,465.18)	2,146,752.43
17	7,026.50	3,572.69	12,764,113.84
18	978.00	(2,475.81)	6,129,635.16
19	1,654.54	(1,799.27)	3,237,372.53
20	3,066.00	(387.81)	150,396.60
21	35.87	(3,417.94)	11,682,313.84
22	78.99	(3,374.82)	11,389,410.03
23	2,003.00	(1,450.81)	2,104,849.66
24	6,995.41	3,541.60	12,542,930.56
25	3,915.50	461.69	213,157.66
Sum	86,345.24		392,839,570.23
Average, $\overline{X}$	3,453.81		16,368,315.43
		Std. Dev.	4045.78

of those differences. Following the formula, dividing the sum of these squared differences by the population size minus 1 (a correction because this is a sample) will compute the standard deviation here of $4,045.78.

The properly skeptical internal auditor may ask: "What is all of this good for?" Standard deviation is a measure of the central tendency of a normally distributed population of data, and it shows how far the items in a population are from the mean or central point. A population of 50 items all with values of about $1,000 each as well as a population of another 50 with average values of less than $1 would have about the same mean value as a different population of 100, with 50 around $450 and the other 50 of around $550. Although the mean for each would be around $500, they would be very different populations of data, and the standard deviation would help to explain those differences.

- A *normal distribution* is the bell-shape diagram used to show data; often it is organized with a few values very high, a few very low, and most in the middle. If a large supply of small pebbles were to be dropped, one by one, onto a flat surface, the pebbles would form in a mound the shape of a bell curve. Much of the data internal auditors deal with also follows this bell-curve shape. If we look at the population of an average large city and plot the number of people



Distance from mean in terms of ± standard deviations on both sides of mean	Percentage of observations included
±1.00 SD	68.26%
±1.65 SD	90.00%
±1.96 SD	95.00%
±2.33 SD	98.00%
±2.58 SD	99.00%
±3.00 SD	99.73%
±3.30 SD	99.90%

EXHIBIT 9.5 Distribution of Observations around a Standard Deviation

by age, a few will be either very old or newborn at any point in time—with perhaps an equal number less than 5 years and greater than 90 years—but the average or mean age may be about 45. These ages will be distributed into a bell-curve shape in what is called a normal distribution. The assumption that most populations follow a normal distribution is important for internal auditors involved in sampling. Exhibit 9.5 shows a normal distribution where the mean, median, and mode are all the same.

Standard deviation is a measure of how many items in a population are disbursed around the central or mean point in a standard distribution. Statistical theory says that 68.2% of a normally distributed population will reside plus or minus 1 standard deviation around the mean; 95.4% will be within 2 standard deviations. How the items in the population are distributed around those central measures of mean and standard deviation is often of interest to internal auditors. Is there an equal

distribution of large and small values around the central measures? At times, a population will *not* follow this normal or symmetrical shape. If plotted by age, the population of a retirement community would be heavily weighted to older persons. We would say that this distribution by age is *skewed*. Many other business-related populations follow a skewed distribution, with a few items with very large values. It is important for internal auditors to understand if a population of data is skewed to either the right or the left. This distribution of skewed data often causes auditors to modify audit testing and evaluation procedures.

Because of its rather complex-looking formula, standard deviations may not seem that important, and their calculation may seem rather difficult. Various tools are available to perform these calculations, ranging from spreadsheet software to handheld calculators. An internal auditor who needs a better understanding of standard deviation concepts should dig into an old college textbook or refer to a good current statistical textbook.

(b) Developing a Statistical Sampling Plan

- As a first step for audit sampling, an internal auditor should develop a sampling plan that will allow each item in a population to have an equal probability of selection. Doing this involves a much more precise approach than used in judgmental sampling approaches. The plan should attempt to remove any bias in the selection of items to ensure that they are representative of the total population. An internal auditor often faces a challenge here in understanding any large amount of data, whether inventory records, accounts receivable payment histories, actual physical locations of assets, or other types of audit evidence. Statistical sampling allows an internal auditor to pull a representative sample of these data that will allow an audit conclusion over the entire population of data. However, an internal auditor must understand the nature of the data to be reviewed when developing this sample selection strategy.
- **The population (or universe or field to be sampled must be clearly defined** The *population* is the total number of units from which a sample can be drawn, including the scope or nature of items to be reviewed, such as all accounts payable vouchers for a year and the specific characteristics of audit interest. An example would be a large number of accounts payable vouchers where internal audit is interested only in materials purchases. Payables covering other areas—such as travel reimbursements or telecommunications charges—would not be included in this example audit population.
- **The population should be divided into groups if major variations exist between population items.** A population such as a materials inventory often includes only a few items of very high value and many of smaller values. Such a population would be skewed and not follow a normal distribution. When a population covers a few very large or significant items and many others with very small amounts, statistical conclusions based on the entire population often are not as valuable. Internal audit should consider stratifying the sample by placing the smaller set of high-value items in one population and the balance in a separate population, then drawing separate samples from each.
- **Every item in a population must have an equal chance of being selected in the sample.** Every attempt should be made to eliminate bias in a sample selection when there is a lack of availability of particular items of interest. Auditors

are sometimes guilty of bias when deciding to restrict some items from the sample selection even though the audit's conclusions are expressed in terms of the total population. They may decide arbitrarily to ignore some items in a population because of lack of easy access. For example, it is easy to ignore items located on a top shelf in an inventory audit. They will pull the sample from readily available items and then state their audit conclusions as if they had looked at the entire population. If certain items must be ignored for logistical or other valid reasons, internal audit should always reveal that fact when reporting results.

- **There should be no bias in making the sample selection from the population.** Similar to the last situation, an internal auditor may be faced with a population of items stored at both local and remote facilities and only look at ones in the local facility. The auditor can then draw an audit conclusion based only on the items stored locally. Items stored in remote warehouses that have been ignored may have different attributes from the central warehouse items. Sample result conclusions from the local items reviewed may not represent the remote warehouses.

The sampling plan to be used should be clearly documented and discussed with area management, who with their knowledge of the items to be reviewed may suggest adjustments to the sampling plan. The development of a sampling plan is an important for step for any audit sample.

There are four common methods for selecting an audit sample: *random number, interval, stratified,* and *cluster selection*. The latter two are also often referred to as types of sampling, but they are more properly identified as optional selection techniques. The next sections briefly discuss these techniques. An internal auditor should have a general CBOK understanding of the most appropriate technique for use in a given audit situation.

(i) **RANDOM NUMBER AUDIT SAMPLE SELECTION** Items here are selected *at random,* with each in the population having an equal chance to be selected as a part of the sample. In theory, an internal auditor would place all the items from a population into a container (or numbers to identify them), mix them thoroughly, and draw the individual items for the sample from the container. Since this is generally not feasible, the auditor must find other means to draw the random sample. In the past, auditors often used time-consuming and somewhat complex processes. Today, however, an internal auditor can use any of a large number of computer tools to a select random number sample. An Internet search for *sampling random numbers* will reveal a wide variety of adequate software tools, some free or others selling for a small sum. The idea is to have a starting and ending number for all items in the population, determine the sample size, and then select random numbers based on that sample size. This is a convenient process with, for example, a population of 1,000 invoices where it is easy to identify each by a number.

With larger or more complex populations, each item in the population to be sampled should be assigned a unique identifying number, such as the voucher number on a paper document, part numbers for an inventory, or some sequential number. For example, if the population is described on a multipage computer-generated report, items can be identified on the basis of page number and line number per page. An inventory of 1,625 items could be printed on a 30-page report with about 55 lines per page. Since the individual inventory items in such a report

may not be numbered, they can be identified by their placement on this report. The items on page 1 would range from page 1, line 1 (or 0101 to 0155), followed by 0201 to 0255 for the entries on page 2. This scheme will define the items in the population subject to selection.

The size for any such sample selection should be large enough to allow for the condition that some items cannot be selected and must be replaced.

Although many of the major public accounting firms have developed a theoretical minimum sample size for their tests (often 60 or even 30), internal auditors generally should use *no minimum sample size* in their internal audits. An internal auditor may conservatively select a very large sample on the basis of better results, with management more apt to accept the results of a large sample. Alternatively, a small sample size may be sufficient to arrive at adequate conclusions based on a limited amount of work. These internal audit sample-size decisions are made strictly on the basis of audit judgment and the objectives of the audit without regard to formal statistical sampling rules. Since they are formal and often very mathematical, sampling theory rules are beyond the scope of this book and can be better found in an audit sampling text.

A random number–based population selection assumes that most populations follow a standard bell-curve distribution. Because many actual populations do not follow such a normal distribution, a question sometimes arises regarding the feasibility of using audit sampling. Often a population contains a small but significant group of very large items with the remainder having small balances distributed over a wide range. In other cases, most items in a population, whether as errors or not, may be all nearly equal with respect to the audit attribute being examined. They will not follow a standard distribution even though the basis of many of the statistical sampling methods discussed assumes that the distribution is in the form of a normal distribution. There are mathematical techniques to get around nonnormal distributions and still take a valid sample, but they are mathematically complex and not necessary for the typical internal auditor. However, a good method of assuring more accurate results when a sample is drawn from a badly skewed population is to increase the sample size. Mathematical theory says that as the sample size gets larger, the shape of the sampling distribution becomes closer to a normal distribution.

(ii) INTERVAL SELECTION AUDIT SAMPLE SELECTION Another statistically sound technique for selecting sample items is through what is called *interval selection* or *systematic sampling*. This requires the selection of individual items based on uniform intervals from the items in the total population. This technique is especially useful for monetary unit sampling, discussed in Section 9.5, where an internal auditor develops a sample by selecting every *n*th item in the population, such as from an inventory listing. For this type of sampling, there must be a reasonably homogeneous population, in terms of type of item, and no bias in the arrangement of the population that would result in a sample that is not statistically representative.

Interval selection should be related to the size of the sample and the total population. The planned sample size divided into the population size then establishes the interval. Thus, a population of 5,000 and a needed sample of 200 would yield an interval requirement of 5000/200 or every twenty-fifth item. An internal auditor would then examine every twenty-fifth item in the population series with the starting point in the first interval group established on a random number basis. In the event the actual population turns out to be larger than was estimated, a practical solution is to increase the sample by extending the interval selection on the same basis. If the

actual population is less than estimated, it will be necessary to complete the sample through a new interval selection based on the number of items short in relation to the total population size. This problem can be avoided by always having a safety margin through a larger-than-needed sample estimate.

An interval selection where every *n*th item is selected is perhaps the easiest way to draw a sample from a population; however, the very nature of the method introduces the possibility of bias in the sample selection. For example, in a sample of daily transactions with an interval selection of every 30 days, if the starting random number pointed to the beginning of the month, a compliance error that normally took place later in the month might not be detected. The internal auditor could select day 5 of month 1, then move forward on the interval of 30 to perhaps day 6 of month 2 and so on. Based on this start, items from day 15 to about 30 will never be selected. Because of this bias, internal auditors should use caution before using this technique.

(iii) STRATIFIED SELECTION AUDIT SAMPLE SELECTION In a *stratified selection audit sample selection,* a population is divided into two or more subgroups, with each subgroup handled independently as a separate population. Stratified selection is an extension of random selection techniques because either can be applied to the smaller strata of the population. In some cases, 100% of the items in one of the strata may be examined while the others would be subject to random selection. The justification for stratification may be that one stratum has significantly different characteristics, and internal audit may wish to evaluate that subgroup on a more individual and precise basis. Through reducing variability, stratification can decrease the standard deviation and help to reduce sample sizes.

The data presented in Exhibit 9.3 show where stratification might be useful. Internal audit might decide that all items in the population with balances greater than $10,000 should be examined 100%. In a purely random selection, using a random number table and a sample size of 5, none of the three large items might be selected. Using stratification, internal audit could divide this population into two strata: items over $10,000 and items under. The strata less than $10,000 would be subject to random selection, while the strata greater than $10,000 would receive 100% selection.

Populations that have a few items of very high value, such as inventories, accounts receivable, and invoices, are the most common types requiring stratification. Since these high-value items have much greater significance, internal audit may also wish to subject them to higher standards of scrutiny. In other cases, there may be a need for stratification since individual subgroups are processed in different ways, or by different groups, and the nature of the items may call for different standards of audit scrutiny, such as certain inventory subject to theft. Under these conditions, the larger variability in the total population makes a single type of testing and evaluation inapplicable.

Stratified sampling principles have long been recognized, and audit sampling stratification often provides meaningful for a useful statistical measures plus the possibility of smaller sample sizes. Once the stratification selection technique has been adopted and the subgroups are subjected to different standards of audit scrutiny, the results of each evaluation can be used independently, based on the sampling of the separate populations, or can be brought together to support a consolidated conclusion relative to the total population.

(iv) **CLUSTER SELECTION AUDIT SAMPLE SELECTION** Using a sampling approach called *cluster selection,* samples are pulled by systematically selecting subgroups or clusters from the total population. Cluster selection is useful when items are filed in shelves or in drawers, and it is physically more convenient to select subgroups based on the physical shelf area or individual file drawers. The rationale is that the items on particular portions of the shelf areas or in designated drawers are substantially similar in nature and that a sample thus selected will be representative. However, the variability *within* the individual samples is frequently less than the variability *among* the samples. Hence, to offset this lesser variability, it is customary to use a larger sample with the cluster selection approach. A variation of the cluster selection approach, called *multistage sampling,* involves sampling the individual clusters instead of treating the sample population as a single or whole unit.

Assume a population of 60,000 warehouse items located on 2,000 feet of shelves. If internal audit decides to review a sample of 600, the plan might be to divide the population into 20 clusters where each cluster would have 30 items. Since the average number of items on the shelves may be 30 per linear foot (60,000/2,000), each cluster would cover an area of 1 foot (30/30). These individual clusters would then be selected at intervals of 100 feet (2,000/20) and with a random start. Of course, the validity for this type of sample selection depends on the consistency of the population. That is, random number selection or regular interval selection would presumably assure a better representative sample. Cluster sampling is sometimes useful, but it generally is difficult to execute and must be used with care.

(c) Audit Sampling Approaches

An internal auditor can take several audit sampling approaches depending on the audit's objectives, whether it will be based on tests of compliance, financial statement controls, or any special conditions. The three most common approaches are *attributes sampling, variables sampling* (including monetary unit sampling), and *discovery sampling*. *Attributes sampling* measures the extent or level of occurrence of various conditions or attributes—in other words, to assess internal controls. For example, an internal auditor might want to test for the attribute of whether invoice documents have received proper approval signatures. An invoice will either be correctly approved or not—a yes-or-no qualitative condition. Normally, the attribute measured is the frequency of an error or other type of deficiency. The extent of the existence of the particular deficiency, such as improperly approved documents, determines the seriousness of the situation and how internal audit will report its findings and recommendations. Attributes or characteristics can be applied to any physical item, financial record, internal procedure, and operational activity. Attributes sampling often measures compliance with a designated policy, procedure, or established standard, and it is a test for internal controls. A control is determined to be working or not working. "Sort of working" is not an appropriate conclusion. An internal auditor tests conditions in the selected items and then assesses whether the overall population is in compliance with the control attribute.

Variables sampling deals with the size of a specified population, such as account balances or tests in individual sample items. Here the auditor's focus is on "how much" as opposed to the yes-or-no focus of attributes sampling. The objective of variables sampling is to project total estimated quantities for some account or adjustments to the account on the basis of the auditor's statistical sample. Illustrative

would be a sample to estimate the total value of an inventory based on sample results. Variables sampling is concerned with absolute amounts as opposed to the number or extent of a particular type of error.

Two important variables sampling approaches are *stratified sampling* and the now very common *monetary unit sampling*. Variables sampling procedures are closely related to attributes sampling but include additional concepts and calculations. Because of the more complicated nature of variables sampling, a step-by-step analysis is given for single-stage variables sampling. This example is based on a simplified manual estimate of the standard deviation when computer support tools or other information on the standard deviation is not available.

The third type of statistical sampling, *discovery sampling,* is similar to the non-statistical judgmental sampling discussed earlier. Discovery sampling is used when an internal auditor wants to pull a sample from a large volume of data without the statistical processes associated with variables and attributes sampling. The next sections discuss these sampling methods in some detail, but our presentation but does not equip an internal auditor with enough information to become an expert in statistical sampling concepts. Appropriate additional training, experience, and specialized books and computer software tools are necessary. From a CBOK perspective, an internal auditor should have a general understanding of these sampling approaches and which are appropriate to the situation. More skilled help may be needed to perform statistical-sampling based internal audits.

(i) ATTRIBUTES SAMPLING PROCEDURES Attributes sampling is the process of pulling a sample to estimate the *proportion* of some characteristic or an attribute of interest in a population. For example, an internal auditor may be interested in the rate of occurrence of some monetary error or compliance exception that might exist in a population of accounts payable disbursement vouchers. The auditor here would be testing for the number of items that have some type of significant error, not the total monetary value of all of the errors. This type of test is very appropriate for assessing the level of internal control in some specific account and can be a very important approach for Sarbanes-Oxley Section 404 internal controls tests. The starting point in attributes sampling is to estimate an expected rate of errors—that is, how many errors can internal audit and management tolerate? Depending on the items sampled and the culture of the enterprise, this expected error rate may be as little as 0.01% or as large as 5% or even more. Even if senior management states that "no errors" will be allowed in some highly critical operation, all parties often recognize that there may be a small or very small possibility of an error. Depending on the criticality of the operation, such a very small error rate will be accepted. An expected error rate is the recognition that certain types of operations contain errors, no matter how good the other controls and procedures are. If internal audit were to perform a 100% examination of an account but only find a small number of errors—say, 0.5%—it might be difficult to convince management that its controls are weak. Management might expect and tolerate a 1% error rate here and not express much concern at internal audit's findings. In an attribute-sampling test, internal audit must estimate the expected rate of errors in the population sampled, based on management's stated expectations, other audit tests, or just internal audit assumptions.

Along with estimating the expected error rate, internal audit must decide on the acceptable precision limits and the degree of wanted confidence for the sample. In other words, an internal auditor would like to be able to say "I am 99% confident

that the error rate of this account is less than 1%." These estimates will allow an internal auditor to determine the size of a sample that will provide a reliable conclusion regarding the condition tested. This determination is made through statistical methods and can be obtained from various statistical software packages or even from tables found in the some statistical sampling books. These factors provide an initial basis for the size of the sample to be reviewed. The internal auditor now selects this sample and examines the items sampled to determine the number of errors that exist in the sample.

As can be expected, the error rate in a sample is normally higher or lower than the previously estimated acceptable error rate. If lower, the internal auditor has established that the condition tested is safely within the limits selected. If the sample shows a higher error rate, the auditor must determine whether the results are satisfactory and what further action, if any, is needed. Conceivably, the sample can be expanded, but internal audit often feels that there is an adequate basis for arriving at a conclusion. The key to meaningful attributes sampling is to take an appropriate sample and properly develop an audit conclusion based on the sample results.

Attributes sampling, once commonly used by both internal and external auditors, is now used less frequently because of its computational and statistical knowledge requirements. However, attributes sampling remains an effective tool to report to management on the status of some control procedure. The internal auditor who wishes to obtain a greater understanding is encouraged to seek out a detailed book on the subject.

Attributes sampling is frequently used by governmental regulatory agencies, and its results are acceptable in a court of law. Although the process takes more work than the nonstatistical procedures already discussed, when properly performed, attributes sampling will allow the auditor to express an opinion over the presence of some condition with a high degree of statistical authority.

(ii) **PERFORMING AN ATTRIBUTES SAMPLING TEST** Attributes sampling is useful when an internal auditor faces a rather large number of items to be examined and wants to test whether certain controls are working or not working. An internal auditor must first define what is to be evaluated or the specific nature of the compliance tests to be performed, the nature of the sampling units, and the population characteristics. Attributes sampling is a yes-no type of audit test where the item or attribute sampled must be either correct or incorrect; there can be no measures of almost correct or close enough. In a test of the completeness of travel report approvals, for example, enterprise procedures may state the responsible manager must approve all travel reports greater than $100. Thus, any voucher greater than $100 not approved by the responsible manager would be considered a compliance error. Internal audit should carefully define the types of tests to be performed as well as the acceptance and rejection rules. While it is possible to sample for two or more different attributes separately, each statistical test should concentrate on compliance with one such test criteria. If multiple attributes are used in a single test, the failure of any one would mean that the entire item sampled is out of compliance.

The size of the population as well as the auditor's tolerance for errors will impact the number of items to be sampled. If an internal auditor is testing for travel policy compliance and if there is a requirement for manager approval for vouchers over a $25.00 limit, should internal audit treat a nonapproved $25.01 item as an error or

should it allow for a perhaps 5% or 10% exception rate? As much as possible, these decisions or rules should be defined in advance.

In addition, internal audit should have a clear understanding of the number and location of the items to be sampled. If initial plans are to sample *all* travel accounting reports, those reports must be available or readily accessible. If a few items are filed at a remote, international location, internal audit may not be able to sample *all* such reports unless it gains access to the remote, international reports as well as the national items filed centrally. Otherwise, internal audit should reduce the scope of the population sampled and look at only domestic travel accounting reports.

The auditor must first make some preliminary estimates, based on observations and other audits, of what is expected from the sample results and then pull an actual audit sample based on those expectations. For example, if a fairly high level of errors in the population is expected, the auditor's sample should be sufficient to confirm or refute those expectations. Internal auditors need to estimate the maximum tolerable error rate, the desired *confidence level* of the sample, the estimated population error rate, and then the initial sample size. These key attributes sampling parameters are:

- Maximum tolerable error rate
- Desired confidence level
- Estimated population error rate
- Initial sample size
- Selecting the sample to perform audit procedures
- Evaluating the results of the attributes sampling test

(A) Maximum Tolerable Error Rate Statisticians also call the maximum tolerable error rate the *desired upper precision limit*. This is the error rate an internal auditor will allow while still accepting the overall internal controls. The idea is that a typical population may have some errors. In the previously discussed audits of travel expense reports, which were reviewed for departmental management approvals, a realistic internal auditor recognizes that there may be *some* errors, such as the $25.01 vouchers that are above the $25.00 requirement. This is an error an internal auditor might accept but still feel that internal controls are generally adequate.

The maximum tolerable error rate normally is expressed as a percentage that can vary based on the nature of the items reviewed. In the last example, an auditor might accept a 5% tolerable error rate or upper precision limit. In other instances, a smaller or larger estimate can be used, but this estimate should never be more than 10%. Such an estimate indicates major internal control problems, and the resultant attribute sample may provide little further information. If an internal auditor knows that internal controls are very bad, it is of little value to take an attribute sample to verify what the internal auditor has already determined through other audit procedures. Similarly, an internal auditor normally should expect some errors and establish some reasonable value for this rate, perhaps 1% or 2%.

(B) Desired Confidence Level The desired confidence level is a measure of the auditor's confidence on the results of a sample. That is, internal auditors generally would like to have 95% or 98% certainty that the results of the sample are representative of the actual population. An internal auditor will never be 100% certain that a condition exists unless the auditor reviews essentially 100% of the items in the population.

If a population of 100 items contains one error, an auditor might look at a sample of 10 items and find no errors. The auditor may look at 20, 30, 50, or even 90 items and still not find more than that one error. The only way to be 100% certain that the population contains a 1% error rate is to look at 100% of the items. However, an internal auditor typically should look at a much smaller sample and still be able to state that he or she is 95% or 98% certain that the error rate is no more than 1%.

The assumed confidence level value, usually 95% or 98%, along with the estimated population size, will determine the size of the sample needed to test the estimated population. Too large of a confidence level may require too large of a sample. Too low of a confidence level may reduce the size of the sample, but the results may be questionable. Management typically would not accept an internal audit finding that states they are "75% confident" that some condition is true.

(C) Estimated Population Error Rate In attributes sampling, an internal auditor estimates the level of errors in the population and then takes a statistical sample to confirm or refute those assumptions. In order to calculate the sample size, the internal auditor also needs to estimate the expected rate of occurrence of errors in the population. This estimate, together with the confidence level and the maximum tolerable error rate, determines the size of the sample. For example, if the confidence level is 95% and the maximum tolerable error rate is 5%, the auditor should look at a sample of 1,000 items in a very large population if the estimated population error rate is 4%. A smaller estimated population error rate will reduce the sample size. Given the same parameters, an estimated population error rate of 1% will drive the sample size down from 1,000 to 100 items. If the expected population error rate is very large—greater than 50%—the required sample size will become very large. Generally, the larger the difference between the maximum tolerable error rate and the estimated population error rate, the smaller the necessary sample size.

(D) Initial Sample Size The last three factors, along with some other correction factors, determine the necessary sample size. While calculation formulas can be found in a statistical textbook, internal auditors normally use audit software to develop attributes sampling plans. A Web search for *attributes sampling software* will provide a wide range of options. Accessing such a statistical sample software package, an internal auditor needs to provide only the (1) maximum tolerable error rate, (2) confidence level, (3) estimated population error rate, and (4) approximate sample size. The software then provides the required sample size for the attributes test. Exhibit 9.6 contains some attributes sample sizes estimated using these values. The exhibit illustrates that if the confidence level is 99%, the maximum tolerable error rate is not over 5%, and the estimated error rate is 4%, an internal auditor should examine 142 items for an attributes test over a population of about 500 items.

This is a brief introduction to the process of selecting a sample size when performing an attributes test. A real difficulty for many internal auditors here is that attributes sample sizes tend to be large. When judgmental tests sample perhaps only 50 items, it may be difficult to justify the larger sample sizes needed to perform a statistically correct attributes test. While in some instances an internal auditor can reduce a sample size by modifying sampling assumptions, this may change the overall audit conclusions. Looking again at Exhibit 9.6, with a 1,000-item population and a desired reliability of 3%, an internal auditor will have to pull a sample of 260 items in order to express a 99% sample results opinion with an expected error rate

EXHIBIT 9.6 Attributes Sampling Sample Size Examples

	Sample Size Relaibility of:					
Population Size	+/− 1%	+/− 1.5%	+/− 2%	+/− 2.5%	+/− 3%	+/− 4%
200						99
250						110
300						119
350					175	126
400					187	132
450					197	137
500					206	142
550				263	214	145
600				274	221	148
650				284	228	151
700				293	234	154
750				302	239	156
800			397	310	244	158
850			409	318	248	160
900			420	324	252	162
950			431	330	256	163
1000			441	336	260	165
1050		419	450	341	263	166
1100		422	459	346	266	197

Confidence Level: 99%
Expected error rate not over 5%

not over 5%. This sample size will become much smaller if the confidence level is lowered from 99% to 95%. In such cases, there is the possibility that management may question audit findings with a 95% certainty, particularly when the auditee disagrees with the findings and is looking for a way to refute the sampling results.

(E) Selecting the Sample to Perform Audit Procedures. Having made some audit sample assumptions and determined the sample size, the next step is to pull the actual items for review. The random sampling procedures described previously can be used to select items to review. Multiple attributes also can be tested using the same set of sample items. The point to remember is that an internal auditor will be performing a separate yes-or-no type of test for each of the individual attributes on each of the items in the sample.

Workpaper documentation should describe all items selected as part of the attributes test. Spreadsheet software is useful here for recording the results of the audit tests, but internal audit procedures should be performed with great care. If an audit fails to recognize an error condition in the selected sample items, that fact will throw off the conclusions reached as part of the overall sample. With a large population, each sample item may speak for hundreds or even thousands of actual items. Each sample item should be evaluated carefully and consistently against the established attributes. An assessment of close enough should not be used. If some attribute measurement is too stringent for certain items, internal audit should consider reevaluating the entire sample set. An internal auditor may be looking for several

error conditions but then find another error not included in the original test design. If significant, internal audit may want to redefine the overall attributes test.

(F) Evaluating the Results of the Attributes Sampling Test As discussed, prior to actually selecting and evaluating the sample items, an internal auditor will have made initial assumptions regarding the maximum tolerable error rate, reliability, and level of confidence, as well as about how many compliance errors would be tolerated to assess whether the controls are adequate. The next key step is to evaluate the sample results against those assumptions to determine if an internal control problem exists. Recall that an upper precision limit or maximum tolerable error rate and a confidence level formed the standards used to determine the sample size and perform the sampling test. An internal auditor should now assess the actual error rate of the sampled items and calculate an upper precision limit based on those sample errors. That precision limit, computed on the basis of the actual sample, should be less than or equal to the desired precision limits established at the beginning of the sample exercise in order for the auditor to report favorable results from the sample.

Normally, if the results of the sample do not meet the preliminary criteria, there is a major audit finding. While these audit criteria should have been well thought out and approved before beginning the test, sometimes internal audit or management may decide that the original assumptions were too conservative. A new upper precision limit or confidence level could be used and the sample results measured against it. This approach should be used only with the greatest caution. In effect, the auditor here is attempting to justify some bad results. Were the matter ever to reach a court of law, internal audit would have a tough time justifying why it had altered its assumptions to make the sample results look good. A better approach when the results are unfavorable is to expand the sample size.

When attributes sampling results turn out unfavorably, management sometimes claims that internal audit only looked at some very unusual items and that the remainder of the population is not that bad. An increase in the sample size will have the effect of decreasing the computed upper precision limit, assuming that the auditor does not find a substantial number of additional errors. However, internal audit should weigh the relative costs and benefits of this approach. A better approach is to report the internal control problem based on the current results and to expand the sample size in a subsequent audit review. It is hoped that management would take steps during the interim to improve internal controls in the area of interest.

Attributes sampling is a very useful technique for assessing one or several internal controls in an area of audit interest. Because estimates of such things as the maximum tolerable error rate are made in advance, it is difficult to dispute the audit test assumptions when compared to sample results. Similarly, because random numbers or similar techniques typically are used to select the sample items, it would be difficult to claim auditor bias in the selections. To better explain the attributes sampling process, an example follows.

(iii) ATTRIBUTES SAMPLING AUDIT EXAMPLE This section discusses an example of attributes sampling at Gnossis, Inc., a large research and development sample enterprise. We assume that management has asked internal audit to assess whether the controls over its human resource records are correct. Certain employees have complained that they did not receive their scheduled increases on a timely basis, and Gnossis was recently fined in a court action when human resources records

deficiencies were found during a legal discovery action. Senior management has asked internal audit to review payroll department internal controls.

Gnossis has about 4,000 employees, and internal audit has decided to perform an attributes test to assess the internal controls covering human resource records. The Gnossis human resources function uses two information technology (IT) systems for employee records—one for pay calculations and one for benefits—and also maintains a desktop spreadsheet-based system for such matters as employee health insurance declarations. Through a review of the human resources record-keeping process, internal audit found some 30 different record-keeping control issues, ranging from such major matters as whether pay is properly withheld for tax purposes to more minor items such as whether monthly deductions to pay for an employee recreational activities employee club are correct. Internal audit has combined all of these 30 record-keeping issues as a single attribute, as a single yes/no test. The problem here is that a few minor problems would force internal audit to conclude that internal controls are not working even though no problems were found over the major issues. Often such findings are difficult to communicate to management.

A strategy is to test Gnossis human resource records for separate attributes. Although internal audit could have tested separately for all 30 attributes, a better approach is to decide which are the most significant and to test only for those separate attributes. Assume that internal audit has decided to test human resource records for five attributes:

1. Pay grade and status on the automated system should be the same as in manual files.
2. Authorizations for withholdings should be signed and dated by employees.
3. Pre-employment background checks should have been completed.
4. If there were no life insurance deductions, employee-signed waivers should be recorded.
5. Pay increases are according to guidelines and are properly authorized.

While these are certainly not all of the areas where audit can test to determine if controls are adequate, in this example, internal audit has determined that it will statistically test employee records internal controls based on these five attributes. Internal audit would first discuss this approach with Gnossis management to obtain their consent. The next step is to establish sampling parameters and develop a sample plan. Based on the prior year's experience and staff projections for the coming year, it was estimated that there would be approximately 4,000 employees in Gnossis payroll records. Using statistical sampling software, internal audit assumed an expected error rate of 2%, a desired precision of 1.25%, and a 90% confidence level to select a sample size of 339 items. The item of interest here would be an employee payroll file, and internal audit would separately review employee files for each of these five attributes.

Internal audit's next challenge is to select the 339 plus perhaps 40 extra payroll files for audit inspection. The physical records are stored alphabetically in the human resource department with eight-character employee numbers that are not sequential but assigned when an employee joins the enterprise. Because of turnover over the years, internal audit was not able to directly select the sample by matching selections from a random number table to a list of employees in sequence by their employee number. Rather, the sample employees were selected from a printed list

EXHIBIT 9.7 Attributes Test Worksheet for Human Resources Test of Records

Random Number Selected	Matching Employee #	Employee Name	Audit Attributes Test Result					Auditor Initials	Date Reviewed
			# 1	# 2	# 3	# 4	# 5		
0137	0266812	Archer, James Q.							
0402	0342201	Aston, Robert							
0988	0466587	Djuruick, Mary Jo							
1003	0502298	Eggbert, Katheran P.							
1256	0629870	Fitzgerald, Edward K.							
1298	030029	Gaddi, Emron							
1489	0687702	Horen, Rupert D.							
1788	1038321	Issac, Stanley L.							
1902	1189654	Jackson-Smith, Susan							
2263	1250982	Jerico, John							

of employees, a report 75 pages long and with about 55 items per page, using four-character random numbers 0101 through 0155 by page to 7555.

The sample items selected were listed on spreadsheets, as shown in Exhibit 9.7, with space to list the results of each attributes test. Although largely manual procedures were used to select the sample, internal audit could have made this selection using this automated procedure:

1. Use a random number program to generate 379 numbers for the 339-count desired sample size, along with 40 extras. The range of the random number should be between 1 and 4,000.
2. Output the selected random numbers to a file and sort them in ascending order.
3. Using desktop software, match the sequential random numbers with the record counts on the employee master file. Thus, if the first random number is 0137, the program would select the 137th record on the employee master file.
4. Output the selected record data to a spreadsheet file similar to the data shown in Exhibit 9.8.

This automated approach to attributes sample selection will take more initial effort and is best if internal audit also is contemplating additional audit sampling procedures against the employee records files. Once the statistical sample is selected, these attributes are tested by pulling the designated employee personnel file. The procedures here are essentially the same as for any audit. The internal auditor checks each employee record selected against each attribute and then indicates on the worksheet whether the attribute is in compliance. After reviewing these attributes for the 339 sample items, the final step is to tabulate the exceptions or error rates. For Attribute 1, as described, internal audit finds that 10% of the employees in the sample had data errors between their manual payroll files and automated payroll records. At the 90% confidence level, this represents 7.3% to 13.3% of the total number of employees at Gnossis. Because sample results show an extensive error rate for this one important attribute, the results should be disclosed to management immediately without the need for further sampling.

EXHIBIT 9.8 Attributes Test Worksheet for Human Resources Internal Controls

Random Number Selected	Matching Employee #	Employee Name	Audit Attributes Test Results					Auditor Initials	Date Reviewed
			# 1	# 2	# 3	# 4	# 5		
0137	0266812	Archer, James Q.	*OK*	*OK*	*OK*	*OK*	*OK*	*RJK*	*11/16*
0402	0342201	Aston, Robert	*NO - 12.3*	*OK*	*NO - 14.02*	*OK*	*OK*	*RJK*	*11/17*
0988	0466587	Djuruick, Mary Jo	*OK*	*OK*	*NO - 14.12*	*OK*	*OK*	*RJK*	*11/16*
1003	0502298	Eggbert, Katheran P.	*OK*	*OK*	*OK*	*OK*	*OK*	*RJK*	*11/16*
1256	0629870	Fitzgerald, Edward K.	*OK*	*OK*	*OK*	*OK*	*OK*	*RJK*	*11/16*
1298	030029	Gaddi, Emron	*OK*	*NO - 13.2*	*NO - 14.32*	*OK*	*OK*	*RJK*	*11/16*
1489	0687702	Horen, Rupert D.	*OK*	*OK*	*OK*	*OK*	*OK*	*RJK*	*11/16*
1788	1038321	Issac, Stanley L.	*OK*	*OK*	*OK*	*OK*	*OK*	*RJK*	*11/16*
1902	1189654	Jackson-Smith, Susan	*OK*	*OK*	*OK*	*OK*	*OK*	*RJK*	*11/16*
2263	1250982	Jerico, John	*NO-12.5*	*OK*	*OK*	*NO - 25.23*	*OK*	*RJK*	*11/16*

Summary information on the results of these five attributes tests would be provided to management in a formal audit report, as discussed in Chapter 17. Only minor or insignificant problems appear for three of the five attributes tested, while for the other two, Attributes 1 and 3, significant internal control problems are found. In internal audit's opinion, the internal control breakdown over these two attributes is sufficient to suggest major problems within the human resources record-keeping process. Based on these internal audit recommendations, management should analyze the entire file to determine the extent and frequency of these and other attribute errors throughout the system.

(iv) ATTRIBUTES SAMPLING ADVANTAGES AND LIMITATIONS When there is a need to review a large number of items, attributes sampling procedures can provide a statistically accurate assessment of a control feature or attribute. Although statistical theory requires a relatively large sample size, internal audit can review some control or condition within a sample of that data and then can state that it is confident, within a preestablished confidence value or percentage, that the number of errors in a total population will not exceed a designated value or that the control is working. Attributes sampling is not useful for determining the estimated correct value on an account, such as an inventory book value, but is an extremely useful tool for reviewing control procedures in a variety of operational areas. For some internal auditors, the technique has some impediments to its use, including:

- **Attributes sampling computations are complex.** This chapter has introduced some very basic attributes sampling concepts. The actual review and analysis of sample results can be very complex and may require the use of specialized audit sampling software. An internal auditor needs to have a good understanding of the process or could be in danger of interpreting results incorrectly.
- **Appropriate definition of attributes may be difficult** In the previous human resources records example, internal audit sampled and evaluated controls on five attributes selected from a set of 30 actual attributes. The selection of attributes to be tested was based on either auditor judgment or management requests. However, an auditor may have missed one or another important attribute when analyzing the data.
- **Attributes sample results may be subject to misinterpretation.** Properly presented, the results of an attributes sample should be stated very precisely, such as "We are 95% confident that the percentage of error items in the account is between 2% and 7.3%." Despite this precision, people may hear these results and interpret them incorrectly, such as "Does this mean there is over a 7% error rate in the account?" That is not what was communicated, but many listeners prefer easier answers.
- **Imperfect data require corrections.** The basic theory surrounding an attributes sample assumes that the population of data follows a normal distribution, with no other unusual complications. While nonstandard data distributions can be corrected through adjustments in sample size selection and evaluations, nonnormal distributions complicate the process.

Despite these problems, attributes sampling provides internal audit with a very powerful tool to assess internal controls in a large population of data through the evaluation of a limited sample. While the technique is too time consuming or

complex for many audit problems, an internal auditor should develop a basic understanding of attributes sampling and make use of it when appropriate. The technique is particularly appropriate when the initial, judgmental results of an internal controls review indicate problems in an area and when management disputes the preliminary results from audit's limited, judgmental sample as being "unrepresentative." A follow-up attributes sample will allow internal audit to take another look at the data and come back making a stronger statement about the status of internal controls surrounding the area in dispute. A general knowledge of attributes sampling should be part of an internal audit's CBOK.

9.5 Monetary Unit Sampling

Attributes sampling measures the extent of some condition, and variables sampling estimates the value of an account. Variables sampling can be further divided into the more traditional stratified sampling methods, mentioned briefly in this chapter, and what is frequently called *monetary unit sampling*. Monetary unit sampling is a technique to determine if a financial account is fairly stated, and it is a good method for estimating the amount of any account overstatements. This technique is alternatively called monetary unit sampling, dollar-unit sampling, or probabilities proportional to size (PPS) sampling. The concept is that every dollar or unit of currency in an account is treated as a member of the population and each has a chance of selection. A $1,000 voucher for an account will have 1,000 units of population while a $100 voucher for the same account will have 100. Thus, a $1,000 item in a population has 1,000 times greater chance of sample selection than a $1 item. This is a very popular form of sampling for public accounting firms. Although various texts and sources use different names, here we call this approach monetary unit sampling.

As stated, the sampling unit is *each currency unit* rather than physical units, such as invoices or payroll checks. For example, if purchases are being tested for a year, the monetary unit sampling population will consist of the total dollar value of purchases made, and the sampling unit will be each dollar of purchases. If errors are found in the invoices, they are related to individual dollars in these invoices using various evaluation methods. A good source for more information on monetary unit sampling can be found in *Audit Sampling* by the American Institute of Certified Public Accountants (AICPA) or in an older, now out-of-print book by Leslie, Teitlebaum, and Anderson,[2] which provides one of the more detailed descriptions of this process. These authors can be considered the fathers of monetary unit sampling for auditors.

(a) Selecting the Monetary Unit Sample: An Example

Assume that internal audit wants to review a series of accounts receivable balances to determine if they are fairly stated or recorded. Also assume there are 1,364 items or customer balances in this example account, with a total recorded balance of $54,902.25. The balances range from some that are large to others that are very small, with the first 30 of them listed in Exhibit 9.9. Assume that internal audit initially has decided on a sample size of 60 or to look at only 60 individual dollars, as discussed in our introduction to this approach, and the items these dollars represent. With this

EXHIBIT 9.9 Monetary Unit Sampling Selection Example

Acct. No.	Balance	Cum. Total	Start	Int. Tot.	-I-Mus Selects			-II-
1	$123.58	$123.58	37 +	124 =	161			
2	$754.22	$877.80	161 +	878 =	1039 SELECT	1039 −	915 =	124
3	$588.85	$1,466.65	124 +	589 =	713			
4	$2,055.95	$3,522.60	713 +	2056 =	2769 SELECT (2)	2769 −	1830 =	939
5	$341.00	$3,863.60	939 +	341 =	1280 SELECT	1280 −	915 =	365
6	$855.20	$4,718.80	360 +	855 =	1215 SELECT	1215 −	915 =	300
7	$12.55	$4,731.35	300 +	13 =	313			
8	$89.00	$4,820.35	313 +	89 =	402			
9	$250.00	$5,070.35	402 +	250 =	652			
10	$1,099.30	$6,169.65	652 +	1099 =	1751 SELECT	1751 −	915 =	836
11	$87.33	$6,256.98	836 +	87 =	923 SELECT	923 −	915 =	8
12	$788.99	$7,045.97	8 +	789 =	797			
13	$5,892.10	$12,938.07	797 +	5892 =	6689 SELECT (7)	6689 −	6405 =	284
14	$669.90	$13,607.97	284 +	670 =	954 SELECT	954 −	915 =	39
15	$24.89	$13,632.86	39 +	25 =	64			
16	$123.00	$13,755.86	64 +	123 =	187			
17	$123.00	$13,878.86	187 +	123 =	310			
18	$6.00	$13,884.86	310 +	6 =	316			
19	$540.90	$14,425.76	316 +	541 =	857			
20	$100.50	$14,526.26	857 +	101 =	958 SELECT	958 −	915 =	43
21	$66.89	$14,593.15	43 +	67 =	110			
22	$39.00	$14,632.15	110 +	39 =	149			
23	$35.00	$14,667.15	149 +	35 =	184			
24	$89.00	$14,756.15	184 +	89 =	273			
25	$100.00	$14,856.15	273 +	100 =	373			
26	$53.90	$14,910.05	373 +	54 =	427			
27	$436.09	$15,346.14	427 +	436 =	863			
28	$237.76	$15,583.90	863 +	238 =	1101 SELECT	1101 −	915 =	186
29	$209.91	$15,793.81	186 +	210 =	396			
30	$28.89	$15,822.70	396 +	29 =	425			

Starting Random Seed = 37
Interval Selection = 915
Total Sample Items Selected = 10

sample, the internal auditor can look at $54.902.25/60 = $915.034, or every 915th dollar in the account balance. Each time the items included in one of those monetary units are selected, the auditor will examine that entire item.

Exhibit 9.9 has columns for the account numbers (here numbered from 1 to 30), the balance for each of these accounts, and the cumulative total. The additional columns in this exhibit show the process of making a monetary unit selection:

- Although the auditor will select every 915th dollar, a starting point is needed somewhere between $1 and $915. To select this, a starting random number between 1 and 915 was selected; in this case, the number was 37.
- The starting random number, 37, is then added to the first invoice of $123.58 or rounded to 124 to yield 161. (All values have been rounded to avoid pennies.)

Since 161 is less than 915, the next item, 754, is added to the accumulated value to yield 1039. Here the auditor will encounter the 915th dollar, and this item will be selected for review.

- A new starting number is now needed, and 915 is subtracted from 1039 to compute a starting number for the next item of 124. This is added to the third item of 589 to yield 713, not enough for selection.
- The fourth item in this sample is large, 2056. The interval of 915 appears twice in this stream of dollars ($915 \times 2 = 1830$), and the item is selected to represent two of the sample items.
- The sample selection procedures are shown in Exhibit 9.9. The auditor can walk through these calculations using a pocket calculator.

The selection of items for a monetary unit sample is generally just as easy as that shown in Exhibit 9.9. An internal auditor can select a sample using a spreadsheet software package or even through a manual calculation using a calculator. The purpose is simply to determine the monetary interval based on the calculated sample size. Two key points and limitations of monetary unit sampling should be mentioned here. First, monetary unit sampling is useful only for testing for the presence of *overstatement*. In the extreme, monetary unit sampling will never select an account that has been incorrectly recorded at a zero value. If the auditor has selected dollars in a population that is understated, the selection method may never find those dollars. Second, the selection method described does not handle credit amounts correctly. The sample selection procedure would not work correctly if the account included a large number of credit items. The best solution here is to pull out all recorded credit balances and treat them as a separate population to be evaluated. If there are only a small number, they might be ignored. Despite these limitations, monetary unit sampling is an effective way to evaluate the recorded balance in a large monetary account.

(b) Performing the Monetary Unit Sampling Test

The number of dollars to be examined in a population determines the auditor's sample size. Similar to attributes sampling, a monetary unit sampling test requires that four things be known regarding the account to be sampled:

1. The maximum percentage of the recorded population value that the auditor will tolerate for errors. This is the same upper precision limit discussed previously for attributes sampling.
2. The expected confidence level.
3. An expected error rate for sampling errors.
4. The total recorded value of the account to be evaluated.

The first item on the list is the dollar value of the populations that may contain allowable errors divided by the recorded book value of the population. This is the same estimate discussed previously for attributes sampling, an error rate that an internal auditor could tolerate and still accept the overall controls in the system. Using public accounting terminology, an internal auditor should first think of the total amount of *material errors* that would be accepted. Although this can be calculated, generally a small percentage rate of perhaps 2% is used.

The estimated confidence level follows the same general rule for attributes. An internal auditor cannot really say that he or she is *100% confident* unless the sample size is 100%. Too low of a confidence level, such as 80%, will cause management concern. Often 98% or 95% are good assumptions. These factors provide data to determine the recommended sample size, which again can be obtained from a table or from statistical sampling software. The values in Exhibit 9.8, based on a 95% confidence level, can be used here. As discussed previously, this is also an area where some public accounting firms have used a fixed sample size of 60 or sometimes 30, arguing that the mathematics does not require larger sample sizes.

The monetary unit sample size is then used to calculate the monetary interval by dividing the recorded book value of the account by the sample size to determine every *n*th dollar interval. This interval sets a selection limit for larger items, and all items greater than or equal to this interval will be selected. Each item represented by a selected dollar is then evaluated by the auditor to determine if it is correctly stated. The auditor calculates the correct amount for each selected account and records both that amount and the correct audited amount. This will point out how much each account is overstated.

(c) Evaluating Monetary Unit Sample Results

Monetary unit sampling is a popular approach for evaluating account balances to determine if they have been overstated. Since every dollar in every item in an account will be subject to sample selection, overstated items may be discovered during the sampling process. The evaluation of the monetary unit sampling results to estimate the total error in the account is a more complex process. The basic idea is to document the recorded amounts and the audited amounts for each item selected and then to calculate the error percentage for each. Upper precision limits are calculated for each error item to determine the suggested amount of any audit adjustment.

The computations for a formal monetary unit sample evaluation have a series of statistical or theoretical options that go beyond the scope of this chapter. The process is often of more interest to external auditors, who can use this to propose a formal adjustment to a client's audited financial statements. For internal auditors, it is often sufficient to use the results of items selected through monetary unit sampling to gain an overall assessment as to whether an account is correctly stated. Books such as the more recent AICPA publication and Leslie, Teitlebaum and Anderson's[3] can walk the interested internal auditor through this formal sample evaluation process.

(d) Monetary Unit Sampling Advantages and Limitations

The most important advantage of monetary unit sampling is that it focuses on the larger-value unit items in a population. A purely random sample could bypass large-dollar-value items based on a random selection. Because monetary unit sampling selects sample items proportional to their dollar values, there is less risk of failing to detect a material error since all the large-dollar units are subject to selection based on the size of each. Any item in a population that is larger than the monetary interval will *always be selected*. Even though management will expect internal audit to take unbiased, random samples, it might express concern if an audit bypassed certain large-value items using other sample selection techniques. Monetary unit sampling assures there will be a greater coverage of the larger-value items in a population. Another

advantage is that if no errors are found in an initial sample and a very low expected error rate is established, relatively small sample sizes may be used. An internal auditor can readily determine the maximum possible overstatements and restrict the sample sizes in these circumstances. As discussed, public accounting firms often limit their monetary unit sample sizes to either 60 or 30 items. In addition, an internal auditor obtains the benefits of unlimited stratification by use of a monetary sampling unit.

Monetary unit sampling is also attractive because the item selection is computationally easy. As illustrated in the previous example, an internal auditor can select a sample from a relatively large population using a spreadsheet program or even a pocket calculator, making it a good choice when at a field location and lacking computer-assisted audit tools. The main disadvantage of monetary unit sampling is that the procedure does not adequately test for financial statement understatements. Missing documents or transactions are a common problem in poorly controlled systems, and if items are missing from a population, dollar-unit sampling procedures will not detect the missing items. They cannot be sampled. Accordingly, an internal auditor cannot project a value of the population using monetary unit sampling. A drawback to this method is that zero or negative values cause problems because there is no chance such items will be sampled. Another problem is that a total book value must be known in order to make interval calculations. The method cannot provide estimates of unknown population values. Finally, because monetary unit sampling is a relatively new concept for internal auditors, there are fewer training programs available than for traditional methods such as attributes sampling.

Despite these concerns and limitations, monetary unit sampling is often the best method for auditing errors in some recorded book values. It can also be useful as a selection method for an internal control attributes test when all items in the population have some recorded monetary value. The approach is often superior to the random number selection previously discussed and will result in a very appropriate selection.

9.6 Variables and Stratified Variables Sampling

Variables and stratified variables sampling are methods of audit sampling where the internal auditor's objective is to test the detailed items that support some account total in order to assess whether that total is fairly stated. Although discussed separately because of its characteristics, monetary unit sampling is really a type of variables sampling. In a variables sample, an auditor selects individual *items* in a population and estimates the total population based on whether the items selected were fairly valued. A variation of pure variables sampling is called *stratified sampling*; here a population is divided into levels of extended item value in a population. Similar to the discussion on attributes sampling, items here within each strata are selected, often with different sampling plans for various strata. The highest-value strata may have 100% inspection while the selection for lower-value strata may be based on random selections.

Variables sampling, particularly when using stratification, can require some daunting mathematical calculations. It saw limited auditor use until computer systems and software became available to simplify sample selections and calculate the projection of results. Stratified sampling allows internal auditors to place a greater emphasis on larger items in a population when they are included as separate strata.

However, by placing them in a separate population subject to random selection, the internal auditor will not be forced to examine all of these items, providing a major advantage of improving the efficiency of the testing. When the population variability or standard deviation is high, sample sizes may be reduced for the desired levels of precision and reliability by using stratified random sampling. If a sufficient number of strata are selected, the sampling error often can be reduced substantially. With the use of modern statistical sampling software, this becomes a very feasible internal audit approach. Another advantage is that emphasis can be given to sensitive areas that require potential audit attention. Often an internal auditor's preliminary analysis will disclose areas with potential errors or problems. These can be classified in separate strata and audited 100% or on a sampling basis, as warranted. Stratification provides an internal auditor with a tool for reviewing sensitive areas in a very systematic manner. The computation to perform stratified variables sampling properly is complex and usually requires computer software.

Because mastering the mathematics of variables sampling is often difficult, the internal auditor reader may ask, "Why should I care about this?" A practical example might help. Some years back, this author was involved in an internal audit of the manufacturing inventories at several large facilities. For defense contractual and other reasons, there was pressure by senior management and the external auditors to take a full end-of-year physical inventory although plant management resisted, saying its local inventory cycle counting procedures were strong. An internal audit procedure was developed to survey and stratify inventory records by their extended item values. A variable sample was pulled, test-counted by internal audit, and the results were projected over the total inventory value. The end result was that internal audit was able to report it was 99% confident the plant inventories were between plus or minus X dollars, which was consistent with the recorded inventory book values. Internal audit saved the plants from taking full physical inventories.

We have talked about computer statistical sampling software in a general manner here, not recommending any one package over another because software and related technology change so fast that recommendations could soon be obsolete. For suggestions on appropriate software to use, the internal auditor might contact the IIA, an external audit firm, or perform a Web search.

The real strength of variables sampling comes from an internal auditor's ability to suggest a projected book value for the account sampled. As discussed in the previous example, internal audit can perform a stratified variables sample of an inventory and then report the results to management, stating "We are 95% confident that the correct book value of the inventory should be between X_{LOW} and Y_{HIGH}. Since the recorded book value of the inventory at the time of our sample was Z, we recommended an adjustment of plus or minus W dollars." This is a very powerful internal audit decision tool.

Using variables sampling, an internal auditor can decide how to report the projection of dollar amounts, whether for adjustments or for estimates of the effect of a particular deficiency. The projection is normally stated as a range of values for a given confidence level. Management, however, often prefers a specific dollar amount or point estimate. The point estimate is calculated by multiplying the sample's mean times the number of items in the universe. This estimate generally is used when the range of values, or confidence interval, around the point estimate is small. For example, the point estimate based on a statistical projection of the results of an

audit is $100,000. The precision at a 95% confidence level could be stated as plus or minus $4,000, giving a range of final audit results between $96,000 and $104,000. Under these circumstances, management will accept such a range, and the use of the point estimate generally would be warranted.

If the calculated range were between $60,000 and $140,000, management probably would never accept these results. An internal auditor would have to either increase the sample size or use a different method of reporting. One method of reporting here would be to state: "We estimate with a probability of 95% that the recorded inventory value of $2.5 million is overstated between $60,000 and $140,000, and is most likely overstated by $100,000." The projected results can be presented in terms of the upper limit, where the internal auditor reports the assurance that the amount of error or deficiency is *not greater than* this amount. In a statistical review of equipment on hand, an internal auditor could project, at a 95% confidence level, that the maximum overstatement of the equipment is $30,000. Since this amount is not material in relation to the $5 million of equipment owned by the enterprise, the auditor can conclude that the amount of error is not significant.

However, an internal auditor could also analyze the causes of errors found in the sample to determine procedural weaknesses that require correction. Internal audit frequently uses the upper limit to determine the validity of account balances for financial statement purposes. A tolerable error rate is first determined for the population. If the projected error rate using the upper limit does not exceed the tolerable error rate, the account is considered reasonably stated for financial statement purposes.

A one-sided confidence limit also can be used to demonstrate that the total universe value *is not less than* some amount at a given confidence level. For example, in a statistical sample of fixed asset acquisitions, it is found that equipment costing over $1,000 was being expensed rather than capitalized. The projection shows a 95% confidence that the amount expensed in error is at least $150,000. Audit samples typically are based on the amounts of individual inventory items. Frequently it is more practical to deal with the differences between the book and actual (as determined by an internal auditor). Under this approach, a similar procedure is followed, but all of the samples and computations pertain to the differences data. The advantage is that smaller amounts (and thus smaller standard deviations)—and, therefore, smaller samples—will be required to achieve the same levels of confidence and precision.

It is, of course, possible that the differences will be as great or almost as great as the absolute values and, therefore, the advantages may disappear. However, the use of differences is a good technique that often can be used as a first approach. A second type of evaluation is the ratio estimate. Here the auditor works with ratios instead of absolute values. Computations of the standard deviations under this method are more complicated, but IT resources can effect significant time savings. Using the ratio estimates method is preferable to the difference estimates method when the errors found are related in size to the value of individual items being tested.

This discussion of variables sampling is very brief and does not describe much of the mathematics typically required in such an exercise and embedded into statistical sampling programs. For more information, an internal auditor should consult one of the previously referenced statistical sampling books. See Exhibit 9.4 for examples of standard deviation calculations.

9.7 Other Audit Sampling Techniques

A fair amount of study, training, or experience is necessary to gain more than a minimum level of proficiency in any of the audit sampling methods discussed in this chapter. Attributes, monetary unit, and variables sampling—probably in that order—are the more important tools for internal auditors to understand and use. An internal auditor should develop a high-level CBOK general understanding of these techniques, but establishing expertise takes some additional work. Sampling, however, is a broad area; other less complex methods can be used under certain circumstances. The next sections briefly describe some of these other internal audit sampling methods.

(a) Multistage Sampling

Multistage sampling involves sampling at several levels. A random sample is first selected for some group of units, and then another random sample is pulled from within the population of the units first selected. For example, assume each of 200 retail stores maintains its own inventory records, sending only summary results to a headquarters office. Internal audit, interested in the age or condition of the inventory, might first select a sample of the stores and then at each store select a random sample of inventory items. When all locations are examined with a sample selected at each location, the result can be treated as a variables or attributes sample.

Multistage sampling assumes that each primary sampling unit is homogeneous, but such assumptions sometimes can cause problems. If an internal auditor assumes that all of the example retail unit stores are essentially the same but subsequently finds that one or two of the units are very different from the others, such a failure to consider those unusual stores in the overall audit test can bias any overall sample projection. While this technique can be useful for a retail chain store environment, the formal mathematics for calculating sample sizes, reliability, and in particular estimating the sampling error is complex. While practical for the chain store situation, the method can break down if the internal auditor wants to project the results of the sample test statistically.

(b) Replicated Sampling

Replicated sampling is a variation of multistage sampling that requires the drawing of one overall random sample of size X, composed of Y separate random subsamples of size X/Y. If a sample of 150 items is to be taken from a very large population, rather than drawing a single sample, an internal auditor might select 15 samples of 10 items each. The auditor would pull these primary samples from the overall population using a series of random numbers. Then the same random numbers used to select each of the primary items are used to select subsamples for items within those groups. The first random number would be assigned to subsample 1, the second to subsample 2, and so forth until a sufficient number had been apportioned.

Why would an internal auditor want to use replicated sampling rather than the multistage sampling previously described? The main reason is that the mathematics is easier. Again, this chapter does not provide a detailed discussion of this sampling procedure, but the technique may be useful to internal auditors in some situations.

(c) Bayesian Sampling

A technique that is rarely used or even mentioned in the audit sampling literature but that appears to have great potential promise is *Bayesian sampling.* The procedure is named after the English mathematician Thomas Bayes and is based on revised probabilities of sample sizes and the like, using what are called *subjective probabilities* acquired from the results of prior tests. Very simply put, Bayesian sampling allows an auditor to adjust sample assumptions and probability factors based on the results of a prior audit. In other words, even though the size of the population is the same and the auditor's risks are unchanged, the sample can be modified based on the results of past audit work. While auditors tend to do this as a matter of course, Bayesian sampling allows an auditor to *formally* modify the sampling plan based on the results gathered in past audit tests.

This section only briefly highlights these audit sampling concepts. Internal auditors probably will not encounter Bayesian sampling in internal audit publications or by contacts with their external auditors. However, detailed reviews of the Committee of Sponsoring Organizations (COSO) internal controls, as described in Chapter 3, could make a Bayesian sampling approach potentially attractive. Internal auditors may encounter Bayesian sampling in the future.

9.8 Making Efficient and Effective Use of Audit Sampling

An understanding of audit sampling is a key, important part of an internal auditor's CBOK, but audit sampling is not an essential part of all audits. An internal auditor may or may not decide to test transactions when performing an audit. The internal auditor decides, on the basis of overall comparisons and other auditing procedures, that a test of transactions is unnecessary or that the amounts involved are not sufficiently material to warrant testing. However, an internal auditor often is faced with situations that will require sampling of transactions. The best control systems cannot eliminate errors resulting from system breakdowns, and overall reviews or tests of a few transactions may not be sufficient to disclose whether internal controls are operating effectively.

While procedures may appear to be adequate, an internal auditor generally must test actual transactions to determine whether those procedures have been followed in practice. If tests are made, audit sampling should be considered as a basis for arriving at more valid conclusions. If the test of transactions generated through the audit sample indicates that operations are acceptable, no further work may be required. Where errors are found, an internal auditor should consider one of the next methods in order to arrive at an audit conclusion:

- **Isolating errors.** Through a review of the types of errors and their causes, an internal auditor may be able to isolate the total amount of errors. For example, one vendor may be submitting erroneous invoices, and a review of all of the vendor's invoices may pinpoint these specific errors. As another example, a particular automated system may appear to be causing the errors, and a special review of that system may be required. Either type of analysis can determine the amount of deficiency as well as the basic cause.

- **Reporting only on items examined.** When an internal auditor encounters significant errors, it may only be necessary to report the results of the tests to operating personnel. The nature of the errors may be such that it is the responsibility of operational managers to strengthen procedures and determine the magnitude of errors. As part of this review, an internal auditor should attempt to determine the causes for the condition and make specific recommendations for corrective action. Unless an internal auditor projects the results of a statistical sample, management is provided only with the errors or amounts pertaining to the items examined but does not see an estimation of their significance over the entire population.
- **Performing 100% audits.** Although an internal auditor is not expected to perform a detailed examination of all transactions, sometimes there may be a need for an extended examination when significant errors are found. An example is where certain recoveries are due from vendors but where specific vendors and amounts have to be identified in order to file the claims. If not a 100% examination, the auditor's sampling plan would have to be based on a very high confidence level, perhaps greater than 99%, and a low risk of perhaps 1%. The result will be a very large sample but with a very high acceptability of sample results. This large sample size or 100% examination may not be justified in terms of the costs involved, and a more conventional statistical sampling plan may suffice.
- **Projecting results of sample.** If the selection of items for the test is made on a random basis, the results can be evaluated statistically. The number and dollar amount of errors can be projected to determine the range of errors in the entire field at a given confidence level. The projection can be used to make an adjustment or as a basis for decisions of the kind described in the preceding paragraphs.

Audit sampling is a powerful internal audit tool to support audit procedures such as inquiry, observation, vouching, confirmation, computation, and analysis. As a basis for extending its use of audit sampling, internal audit should review areas in which testing was performed in prior reviews and analyze the objective of those tests, period covered, the effective use of judgmental or audit sampling, number of items in both the field and the sample, results of these tests, and feasibility of using these audit sampling procedures in subsequent audits.

For many years, audit sampling was a difficult process both to understand and to use. Internal auditors needed to refer to published handbooks filled with extensive tables and then to use these data to perform fairly detailed sample selection and test results calculations. The process was comparatively difficult and was not understood by many internal auditors. IT sampling software has changed all of that. It simplifies the necessary calculations, eliminating the need for reference to formulas or tables, and enables internal auditors to obtain more precise and unbiased results. While an internal auditor can, of course, use the time-consuming manual calculation procedures to determine the sample size and to evaluate results in the rare situation, today's laptop computers contain the tools to make this sampling process much easier. These techniques also facilitate the use of audit sampling for many internal audit procedures:

- **Combine audit steps.** Savings in audit time can be achieved if various audit steps are performed as part of the same statistical sample. This can be done

by testing for as many attributes or characteristics as possible in the sample. For instance, in a review of purchases, the primary audit objective may be to determine whether there is adequate documentary support. In addition, an internal auditor may decide to include statistical sampling tests to determine whether excess materials are being acquired.

- **Use a preliminary sample.** Internal auditors can devote considerable effort to developing a sampling plan based on an estimated confidence level, precision, and expected error rate or standard deviation; however, in many cases there is insufficient information in a first audit to develop the sampling plan. By taking a preliminary sample of from 50 to 100 items, an internal auditor is in a better position to make decisions on the extent of sampling required. The preliminary sample can then be included as part of the final sample, and the results of the preliminary sample may lead an internal auditor to conclude that no further testing is required.
- **Perform interim audits.** When a sampling plan is prepared in advance—such as for the year—the items to be tested can be examined on a monthly or other interim basis without waiting until the end of the year. Thus staff auditors can be utilized when available to perform the audit sampling on an interim basis. For example, if the sample plan calls for examination of every 100th voucher, these can be selected for examination as the transactions are processed.
- **Enlarge the fiel size.** A basic consideration in audit sampling is that the sample size should not vary greatly with an increase in field size. Thus, savings can be obtained by sampling for longer periods of time, or from a field composed of more than one department or division. In some cases, an internal auditor may decide to test a particular account for a two-year period, with selection of items during the first year on an interim basis as part of that two-year test.
- **Use a mix of attributes and variables sampling.** If an internal auditor does not know in advance whether variables sampling is required, and since variables sampling is more complex to apply, the auditor may pick a random sample for attributes, evaluate the results, and then decide, on the basis of dollar errors, whether variables sampling may be required. If variables seem appropriate, the sample can then be projected or incorporated into an extended sample. The important point is that once a sample is taken on a random basis, it can be evaluated using different sampling methods.
- **Apply simple audit sampling methods.** Some auditors believe that they must use complex methods of sampling and spend considerable effort and study in arriving at the method to use. In most instances, a simple estimation sample will provide adequate results, without the need for techniques that are difficult to understand, apply, and explain. An internal auditor should not overlook judgment in the audit tests, and sensitive items should be examined in addition to a random selection of items. These can be examined on a 100% basis or sampled as part of a separate stratum.
- **Achieve an effective balance of audit costs and benefits** An internal auditor should assess the costs of examining each sampling unit when making a decision on extending a sample, with consideration given to the costs of additional work compared with benefits from obtaining increased confidence or precision in the final results. When an internal auditor first tries and then effectively uses some of

the audit sampling techniques discussed in this chapter, he or she subsequently may find other areas to sample in the course of operational audit, including production activity improvements, improved inventory management, or even records and document management.

Audit sampling is a powerful tool that is too often ignored by many internal auditors. At one time internal auditors did not use audit sampling because many viewed it as being too difficult or too theoretical. Auditors found it easier to say "You have a problem here" rather than to say "Based on our audit sample, we are 95% certain that we have identified a control problem." Findings based on appropriate audit samples allow internal auditors to express concerns or opinions on a more solid basis. Automated tools now make statistical sampling a simpler task than in earlier days when auditors relied on extensive tables of values and difficult formulae. Today, the effective modern internal auditor should learn the basics of audit sampling and use them when appropriate. A good understanding of audit sampling should be part of an internal auditor's CBOK.

Notes

1. American Institute of Certified Public Accountants, *Audit Sampling* (New York, 2008); Dan M. Guy, D. R. Carmichael, and O. Ray Whittington, *Practitioner's Guide to Audit Sampling* (New York: John Wiley & Sons, 1998).
2. AICPA, Audit Sampling; Donald A. Leslie, Albert D. Teitlebaum, and Rodney J. Anderson, *Dollar-Unit Sampling: A Practical Guide for Auditors* (Toronto: Copp Clark Pitman, 1979).
3. Ibid.

CHAPTER 10

Audit Programs and Establishing the Audit Universe

With overall objectives to review and improve internal controls as well as to promote the effectiveness and efficiency of operations, an internal audit function has a wide variety of areas and activities to include in its reviews. It can concentrate on reviews of financial process internal controls, operational areas in the enterprise, safety and security issues, controls related to information technology (IT) systems, or any of a series of other areas. Given the broad scope of enterprise operations and management and audit committee demands for internal audit attest services, many internal audit functions find that there are just too many areas to include within their scope, given staff, budget, and timing constraints. Internal audit functions need to define the areas within their scope that they may consider for internal audits. This list of all of the potential areas to audit is often called the *audit universe.*

Although the term *universe* sounds a little space age, the term and concept have been used by internal auditors for some time. With reviews and approvals by the audit committee and senior management, the audit universe is the established population of auditable entities for any internal audit function. Such an audit universe may not cover every unit in the enterprise; some are just too small, low risk, or technically complex to be considered for regular internal audit reviews. However, once an internal audit function has established its scope of potential areas to review, the chief audit executive (CAE) and other members of the audit team can subject areas to risk analysis and otherwise develop overall internal audit activity plans.

This chapter looks at the concept of establishing and maintaining an audit universe for an enterprise's internal audit function as well as using that universe as a basis for outlining high-level internal audit procedures, performing risk assessments, and establishing an effective internal audit program. Our common body of knowledge (CBOK) concept here is that internal auditors at all levels should understand the importance of having an enterprise-specific internal audit universe as a basis to guide their internal audit activities. That audit universe will help internal audit to better present planned activities to the audit committee, as discussed in Chapter 23, and to more effectively plan risk-based internal audits, as discussed in Chapter 15.

In addition, all members of an internal audit function should perform their internal audit procedures in a consistent and orderly manner. They will accomplish these audit procedures through documents called audit programs. While audit programs may follow different formats from one enterprise to another as well as for different specialized internal audit types, they should follow a consistent format within an

internal audit function. All internal auditors should have a strong CBOK understanding of how to use and construct internal audit programs.

10.1 Defining the Scope and Objectives of the Internal Audit Universe

An audit universe is the aggregate of all areas that are available to be audited within an enterprise. To define its audit universe, internal audit should review or understand the number of potential audible entities in terms of both the business units or areas of operations within the enterprise and the number of auditable units or activities within and across those business units. These auditable entities can be defined in a number of ways, such as by function or activity, by organizational unit or division, or perhaps by project or program. Some examples of auditable activities include:

- Policies, procedures, and practices both on an enterprise level and those specific to locations, such as at international units
- Manufacturing, distribution, or supply chain units
- Information systems on infrastructure and specific application levels
- Major contracts or product lines
- Functions such as purchasing, accounting, finance, marketing and mothers

These are examples of the major processes that help drive an enterprise. Some may be centrally directed while others are unique to a specific auditable entity. The idea is to define these processes in a manner such that specific internal audits can be planned and conducted.

The second way of looking at these entities is by business unit. In today's environment, an enterprise may have several lines of business with operations across the globe and may exhibit a myriad of authority/responsibility and reporting structures. In order for an internal auditor not to get lost in the complexity of corporate structures, an organized "inventory" of all significant auditable units should be compiled. The definition of auditable entities units depends on specific organizational characteristics and whether the enterprise is functionally organized or product centered. The idea is not to get too big or—an even greater problem—too small in these definitions. We should define auditable entities in a manner where individual internal audits will be cost effective. Some examples include:

- Consider a multiplant manufacturing facility with many small production units. It might make sense to define all manufacturing processes at each of these smaller production units as potential auditable units. These production plant potential audits would include all manufacturing activities at each facility, such as purchasing, receiving, factory floor routing, quality assurance, shipping, and other individual internal audits. An audit team would not review individual processes, such as receiving, at just one production plant. Internal audit would more typically cover all plant-by-plant manufacturing activities.
- For a multirestaurant chain with many small units, it might be best to define each individual small restaurant as an auditable unit, with no plans to schedule specific processes at each of those restaurants as a separate audit. An internal audit team here might review all operations at a particular restaurant rather than

a common process, such as cash control procedures for all of the restaurant units.

- In many instances, it may be most efficient to designate a common process covering all units as an overall auditable entity, particularly if common policies and procedures cover all individual units.

In building their audit universe description, the CAE and the supporting internal audit team might start with a fairly detailed organizational chart to describe the auditable entity units. This review of organizational units sometimes can be a complex process if the enterprise has many subsidiaries, internationally based units, joint ventures, and the like as well as a complex audit department structure. However, the emphasis should be placed on units where the enterprise CAE has prime internal audit responsibility.

Although there can be many different organizational structures, Exhibit 10.1 shows how auditable entities might be identified in a sample enterprise. The idea is that internal audits should be planned in an up-and-down sense across units in the organizational chart. That is, potential audits can cover all operations in an operating division, a subsidiary unit, a plant facility, or major units under a plant. On a cross-dimension, internal audits could be scheduled across such an organizational chart, covering all functional operations—such as IT security management—for each unit that has similar but common functions.

The internal audit team should also define several audit focal points to ensure consistency in their execution of all potential internal audits. These focal points, which serve as a general outline for audit planning documents and audit work programs, help produce trending reports regarding the status of controls in the enterprise's controls environment.

For example, four typical audit focal points for an information security universe are:

1. IT access controls
2. System security configuration
3. Monitoring and incident response
4. Security management and administration

Similarly, the four audit focal points for an IT infrastructure universe element might be:

1. Structure and strategy
2. Methodologies and procedures
3. Measurement and reporting
4. Tools and technology

Internal audit can share such lists of potential auditable entities with members of management for observations or corrections. This information will help them to compile a tentative audit universe that represents all organizational units or activities in the enterprise where internal audit has prime internal audit responsibility. These are not necessarily current areas where internal audit might schedule a review; rather the list is a potential picture of all enterprise-auditable units from an internal audit perspective.

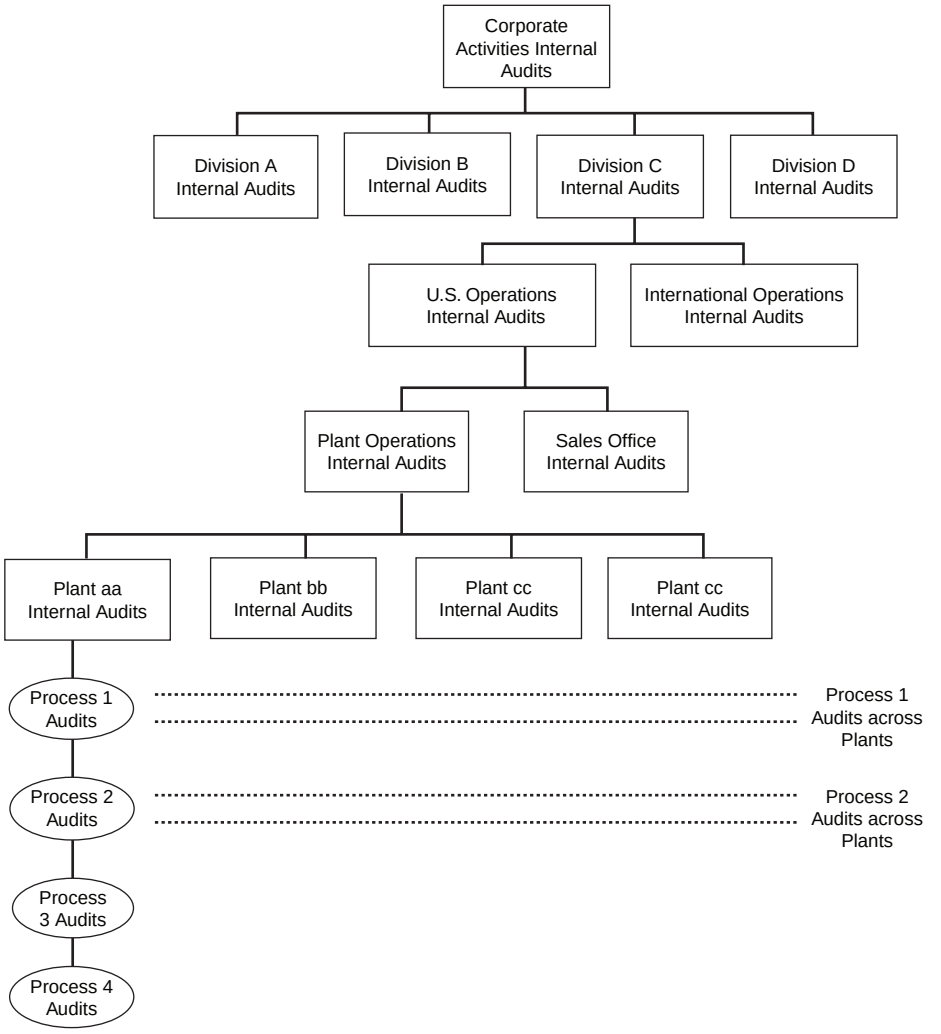


EXHIBIT 10.1 Auditable Entities Organizational Chart Example

This type of picture of enterprise-auditable units is not a one-time exercise; it should be continually maintained and updated as part of annual internal audit planning processes.

To better explain the building of an audit universe, we use our example company, Global Computer Products. Our example company is a hypothetical $2.4 billion sales manufacturer and distributor of hardware and software-based computer security products. It is a medium-size high-technology manufacturing enterprise that is operating internationally. Some other key characteristics of Global Computer Products include:

- **Locations and operations.** The company has a headquarters office in the Chicago area in the United States with a computer security development facility in San Jose, California, and four product distribution centers in smaller U.S.

cities as well as a distribution office in Belgium. In addition, the company has two hardware manufacturing facilities in China and a software production and distribution facility in India. All facilities are leased or licensed, and customer service functions have been outsourced.

- **Management team.** The company's chief executive officer was originally the founder of the company. He and three senior engineers are the only employees left over from the early days and its initial public stock offering. Due to turnover often typical in the industry, most employees have fairly short tenures. The chief financial officer is quite new; the prior officer was asked to resign because of a Sarbanes-Oxley (SOx)–related dispute with the audit committee. The company makes extensive use of nonemployee contract employees. Reporting to the CAE, Global has a relatively small internal audit department as well as a single general counsel.
- **Product description.** Global developed a computer security product that consists of a hardware device plugged into a user's computer USB slot along with software drivers. The hardware device consists of a plug-in card based primarily on standard hardware chips along with some embedded programming. The software is based on proprietary algorithms. Elements of the product design are protected by patents, although these rights have been both challenged in courts and somewhat copied by some competitors.
- **Marketing.** Global's product is marketed by advertisements in professional publications as well as through a team of sales representatives. On a worldwide basis, 80% of sales are to individuals with the balance to smaller businesses. The United States accounts for about 75% of product sales with the balance from Europe. There is also a small but growing segment of sales from Brazil, where an independent agent is distributing the product. By agreement, Global has the right to audit these operations but has never scheduled any work there. Global ships products from its distribution centers direct to computer equipment retailers as well as to individual customers, based on Internet, mail, or telephone orders.
- **Sales and finances** Global's $2.4 billion in sales is split in these categories:

Consumer Cash Sales through Credit Card Purchases	41.0%
Sales to Wholesale Distributors	23.4%
Export Sales to Agents	12.7%
Licensing Fees and Royalties	4.9%

As a relatively young enterprise, its internal audit function does not have a long history of performing internal audits through the enterprise. Rather, internal audit was launched when Global was formed, and most of its initial audit activity has been devoted to accounting and internal controls processes at its Chicago headquarters, some operational process audits at its San Jose distribution, and IT audit reviews of general and application controls at essentially just the U.S. locations. Exhibit 10.2 is an organizational chart for the Global Computer Products sample enterprise.

Global Computer Products had never previously established a formal audit universe statement. It planned and scheduled its reviews based on an informal planning process with management and audit committee requests to perform internal audits in one or another area. One member of the audit committee has been questioning the CAE about the lack of internal audit coverage in several areas, particularly in

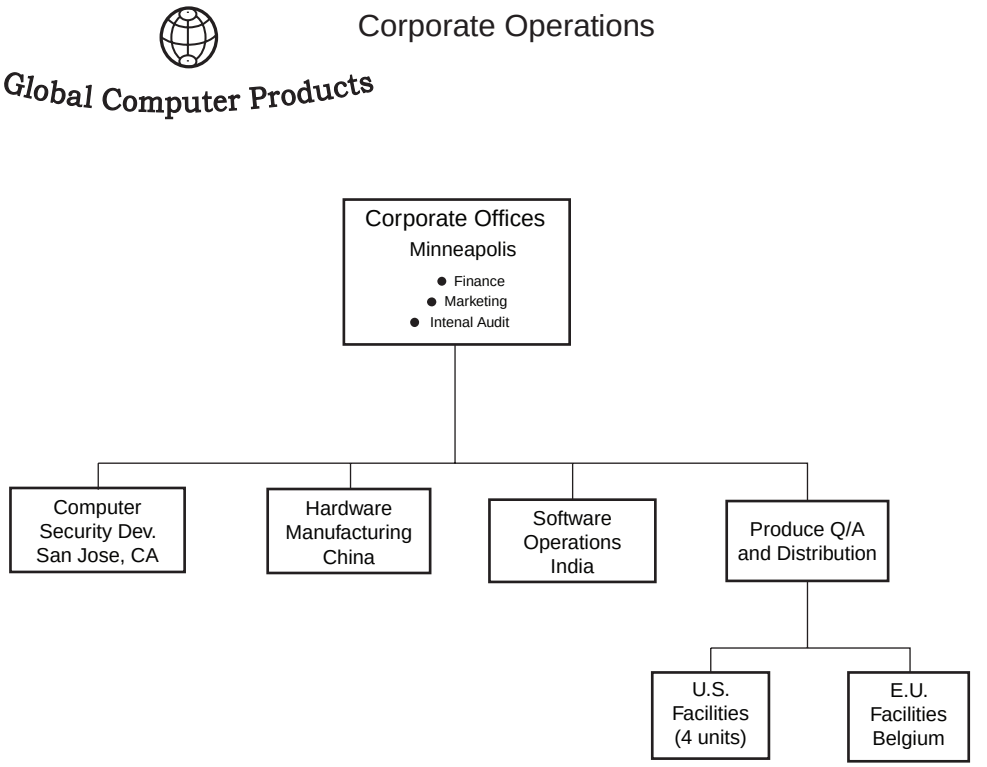


EXHIBIT 10.2 Global Computer Products Sample Organization Chart

international operations. As a result, the Global CAE has made plans to expand internal audit's staff size and coverage.

10.2 Assessing Internal Audit Capabilities and Objectives

A detailed list of enterprise units showing all of the areas that internal audit *could* review is of little value unless internal audit has the skills and resources to launch audits in those areas. This author once joined a large enterprise where the existing internal audit group spent time preparing audit universe lists of all of the entities and units at the enterprise, as part of its annual internal audit planning exercise. The result was extensive and impressive-looking lists of auditable entities, but this internal audit function had neither the capability nor even actual objectives to perform internal audits at some of these units.

This enterprise, for example, had a large group of remote distribution units as well as businesses run by independent franchisees and contractors. An audit universe document included all of these franchisee businesses as auditable units, even though most had never been visited by corporate internal audit. An example of these businesses was a small group of home improvement units whose whole function was to perform home pest removal services. On a contract basis, this franchisee unit would visit a home and remove rats, mice, or bats living in attics.

This relatively small chain of operations had little impact on overall parent enterprise operations. Aside from signing proper contracts and paying commissions to the parent, these franchisees had little connection with parent corporation operations and presented minimal risks. Did internal audit know anything about this type of business? Aside from commission transactions, was there any financial impact? The answer to these questions should have been no. Units like this should never be included on internal audit universe lists.

The idea here is that internal audit should be realistic in developing its audit universe lists. It should develop high understanding of the control risks for each candidate on its universe list and assess whether there are internal audit risks and/or opportunities for each one. Exhibit 10.2 shows a series of European sales and distribution functions for our Global Computer Products enterprise. Although not even highlighted on the high-level organizational chart, assume there is a small office in Kiev in the Ukraine. Since internal audit will almost certainly never visit that unit or have any direct contacts, these Kiev operations do not belong in the audit universe list here. There should only be a note that these units were not included as potential internal audit candidates and the reasons for that decision.

Based on the preliminary list of auditable units and candidates, internal audit should go a step further to develop and enhance its audit resource lists. Although there still may be some uncertainly regarding the nature of some of these business units and their internal control issues, internal audit should analyze each of these potential internal audit candidates in this way:

- **Establish high-level control objectives for each of the audit universe candidates.** The idea is to determine why a unit is on such a list as well as internal audit's potential control objectives for such units. Our previous example of a franchisee household pest control service probably would be eliminated in such an exercise.
- **Assess high-level risks for audit universe candidates.** Following the Committee of Sponsoring Organizations Enterprise Risk Management (COSO ERM) approach discussed in Chapter 6, internal audit should review each of these audit universe candidates and estimate the high-level risks to the enterprise if there was a major internal controls failure associated with the candidate.
- **Coordinate the internal audit activity with other audit and governance interests.** While internal audit is or should be the prime reviewer of enterprise internal controls, any planned audit work should be coordinated with other interested parties. For example, external auditors may request a more complete SOx Section 404 internal controls review, as discussed in Chapter 4, or the human services function may have a need for a Health Insurance Portability and Accountability Act compliance-related review in some area, as discussed in Chapter 26. The audit universe and internal audit planned activities should be coordinated with such external audit requests. Similarly, internal audit projects should be coordinated with planned work by any independent quality audit function, as discussed in Chapter 30. It is easy to say that internal audit should have a lead role here, but these planned audit efforts should be coordinated.
- **Develop high-level control objectives for audits designated by the audit universe.** While this will become more important in an annual planning process, as discussed in Chapter 15, a high-level audit objective should be identified for each item included in the audit universe. This should be a simple statement

of planned audit objectives for each item in the audit universe to help ensure that the strategy, objectives, and scope for each audit includes relevant control objectives (i.e., a completeness check to identify gaps).

- **Develop a preliminary control assessment questionnaire for each audit.** In many cases, items listed on the audit universe are repeats of internal audits from the prior periods. In those situations, this audit guidance should be updated as processes change and reevaluated for future audits in each area. In other cases, internal audit should develop some high-level questionnaires to get started on these potential audit universe reviews.

As a result of this review and analysis work, internal audit should develop a preliminary audit universe schedule that will show the areas for potential review. Such a list would include areas where there is a recurring internal audit interest, where there may be a higher internal control failure risk, and other high-level review objectives. This type of approach will give internal audit a way to initiate its regular internal audit planning activities. Of course, a smaller internal audit group can face a daunting task when building an effective audit universe for a large-scale enterprise. Internal audit may not have the time or resources to perform reviews of items included in audit universe without some other adjustments.

10.3 Audit Universe Time and Resource Limitations

It is sometimes easy to build an audit universe document that includes many—too many—potential internal audits that will never be executed. Our Global Computer Products example illustrates this problem. Global Computer currently has a headquarters-based internal audit group that does not have any international presence. That is, internal audit does most of its work at the home office and rarely travels. Based on the size of this internal audit function, the audit committee should recognize and advise the audit committee that some of the auditable entities on the universe list essentially can never be reviewed, given internal audit's size, scope, and budget. The idea is to demonstrate potential review activities over upcoming periods and what can realistically be included in internal audit's scope of planned activities.

A next step should be to look at the preliminary audit universe list and determine those audits that are required on an annual or a semiannual basis. These are audits, such as SOx Section 404 internal controls update reviews, that must be completed during a current period. Other regular internal audits are not mandated but are expected by senior management and the audit committee. For example, management may expect internal audit to observe the taking of physical inventories in a manufacturing environment. As part of their audit universe and enterprise planning, internal audit should assume that it will need to schedule these reviews on a regular and periodic basis.

Although we are still dealing at a very high level here, a next step is to look at the remaining items in the preliminary audit universe and determine if time and resources are available for reviews of these items. In some situations, there may be just too many audit entity items left in the audit universe to complete over a reasonable period of time. Because of the ongoing enterprise and market changes that we all experience, a time span here should not be more than five years, and

more preferably three years. In addition, these internal audits set for scheduling in the current period or in a three- to five-year cycle may require specialized internal audit skills. More internal audit resources need to be on board for such areas as IT network security or continuity planning and testing. Where additional internal audit skills or resources will be needed, they should be documented and scheduled.

All of these gathered data and planning assumptions will help internal audit to build and publish a preliminary audit universe. This document shows the areas where internal audit plans to perform audits over upcoming periods, the high-level objectives of those audits, and their relative risks. The schedule should also document assumptions: for example, listing audits that will be performed by quality assurance, low-risk reviews that have not been considered, audits that have been eliminated because of logistical difficulties, or audits that will be performed by other bodies. Logistical difficulties often pertain to entities in some fairly distant or difficult-to-schedule location. Our previous mention of the small Kiev office for Global Computer Products is an example. While Kiev is a capital city and certainly not remote, and easily accessed through regular airlines, such a location might present a logistical difficulty for an internal audit review.

Internal audit should prepare an audit universe document for the current period. This document should be reviewed with members of senior management, then presented to the audit committee for approval. Exhibit 10.3 is a portion of a sample audit universe schedule for Global Computer Products. Similar to an annual budget schedule or a capital funding request, this document normally is a much larger, more extensive analysis document. This exhibit is an example of what an internal audit universe schedule might look like.

10.4 "Selling" the Audit Universe to the Audit Committee and Management

The CAE and a key internal audit team may go through massive efforts to build and maintain the internal audit universe and may have solicited the help and advice from senior management in the contents and assumptions of this audit universe, but the audit committee is the entity responsible for reviewing and approving such a document. In the end, the audit committee is responsible if there are any questions regarding why internal audit did or did not look at some area, and the CAE should carefully brief the audit committee members and explain key assumptions.

The audit universe schedule should be prepared and updated on an annual basis for audit committee review and approval. Where the audit committee suggests different areas of emphasis or involvement, the CAE should initiate these internal audit planned changes and make appropriate adjustments to the internal audit annual plan and schedule. In addition, this is often the time for internal audit to seek authorization for changes to internal audit's budget, manpower, or other function changes. Internal audit would be operating under an annual enterprise budget, but it is the audit committee that can make a midstream change—for example, to add a new IT audit staff specialist to the internal audit group.

We have titled this section as the "selling" of the audit universe plan to the audit committee. Perhaps this is an inappropriate term. The audit committee is

EXHIBIT 10.3 Global Computer Products Sample Audit Universe Schedule

Business Unit	Location	Audit Area	Audit	Audit Risk	Prev. Audit	Scheduled
Headquarters	Minneapolis	Financial	Accounts Payable	Low		
Headquarters	Minneapolis	Financial	Banking Operations	Medium		
Headquarters	Minneapolis	Financial	Budgeting	Low		
Headquarters	Minneapolis	Financial	SOx 404 Internal Controls	High		
Headquarters	Minneapolis	Operations	Corporate Marketing	Medium		
Headquarters	Minneapolis	Operations	Advertising	Low		
Product Distribution	Fargo, ND	IT Infrastructure	Inventory System	Medium		
Product Distribution	Meriilville, IL	IT Infrastructure	Inventory System	Medium		
Product Distribution	Los Cruces, NM	IT Infrastructure	Inventory System	Medium		
Product Distribution	Midville, OH	IT Infrastructure	Inventory System	Medium		

responsible for all internal audit activities and should rely on the CAE and other members of internal audit to perform the scheduled audits and to report results back to the audit committee. However, because the typical audit committee does not meet often and may not be close to many changes and new events, the CAE is the individual closest to the audit universe and other changes. The CAE is often the person who communicates changes in internal audit's schedule or in emphasis. The CAE must keep the audit universe and the supporting annual plan in front of the audit committee and also convince, or "sell," approval request concepts to the audit committee for ongoing approval.

The audit universe is the basis for the annual audit plan, as described in Chapter 14, and helps to present internal audit's ongoing activities and performance. Chapter 23 describes audit committee communications and contains some examples of internal audit progress communication with the audit committee. Chapter 13 describes examples of one- and five-year internal audit plans. These are all based on the very important audit universe schedule, a key document that describes internal audit's planned activities over an extended period.

10.5 Assembling Audit Programs: Audit Universe Key Components

An audit universe and its supporting information describe internal audit's high-level review objectives in an area. We have discussed how internal audit should define and document some high-level objectives for each planned review, but it will not be enough to assign internal audit work to a staff-level auditors; they will need some step-by-step guidance to perform internal audits. Internal audits should be organized and performed in a consistent manner with an objective of minimizing arbitrary or unnecessary procedures. To provide help and guidance, internal auditors use audit programs to perform their internal audit procedures in a consistent and effective manner for similar types of audits. The term *program* refers to a set of auditor procedures similar to the steps in a computer program, which go through the same steps every time the process is run. For example, a computer program to calculate pay will include instructions to read the time card file of hours worked, look up the employee's rate stored in another file, and then calculate the gross pay. The same steps apply for every employee unless there are exceptions, such as overtime rates coded into the payroll program. Similarly, an audit program is a tool for planning, directing, and controlling audit work and a blueprint for action, specifying the steps to be performed to meet audit objectives. It represents the auditor's selection of the best methods of getting the job done and serves as a basis for recording the work steps performed.

An effective internal audit department should have a series of generalized audit programs prepared for recurring audit activities. Many of these programs, such as one covering an observation of the taking of physical inventories, are used from year to year and entity to entity with little change. In other situations, the internal auditor may have to modify a standard program to the unique aspects of a particular audit. In some situations, a standard audit program will not be applicable. For example, the internal auditor may want to review controls in a new business entity with some unique control characteristics, or audit management may want to take a different approach because of problems encountered with similar previous reviews. Based on planned audit objectives and data gathered in the preliminary and field surveys,

the in-charge auditor may want to prepare a customized audit program for guiding the review. This may be little more than a standardized program with minimal local changes, or it may be a unique set of audit procedures based on the preliminary planning and the results from a field survey, as discussed in Chapter 7. In order to prepare this program, the internal auditor first should have an understanding of the characteristics of what constitutes an adequate audit program.

(a) Audit Program Formats and Their Preparation

An audit program is a procedure describing the steps and tests to be performed by the auditor when actually doing fieldwork. The program should be finalized after the completion of the preliminary and field surveys and before starting the actual audit fieldwork. It should be constructed with several criteria in mind, the most important of which is that the program should identify the aspects of the area to be further examined and the sensitive areas that require audit emphasis.

A second important purpose of an audit program is that it should guide both less and more experienced internal auditors. For example, management may request that an internal audit department observe the taking of the annual physical inventory. This type of review consists of fairly standard procedures to ensure, among other matters, that shipping and receiving cutoff procedures are proper. A less experienced internal auditor may not be aware of these procedure steps, and even experienced internal auditors may forget one or another. An audit program outlines the required audit steps. An established internal audit department probably will have built a library of programs, established over time, for tasks such as physical inventory observations or reviews of fixed assets. When planning a review where such established programs exist, audit management needs only to use this program while taking into consideration any changed conditions that have been discovered through the preliminary or field surveys. The audit program is revised as necessary, with the changes approved by audit management prior to the start of the review.

For many internal audit departments, appropriate audit programs are not available for many areas. This is because internal auditors typically face a wide and diverse set of areas for review, but they do not have the time or resources to review every area frequently. Established programs prepared for prior audits often become out of date due to new systems or changed processes. The auditor responsible for the field survey or another member of audit management should update any existing audit program or prepare a revised set of audit program steps for the planned review. Depending on the type of planned audit, programs usually follow one of three general formats: a set of general audit procedures, programs with detailed instructions for the auditor, and a checklist for compliance reviews.

Some examples may better illustrate these audit program types. Exhibit 10.4 is an audit program for a review of petty cash controls at a branch unit. It consists of general audit procedures to review cash at any unit of a multifacility organization. Petty cash controls are one of the smaller, less critical internal control concerns in many organizations. However, internal auditors regularly perform this step. The program shows the rather simple steps that should be included in any such audit and illustrates an example audit program.

This audit program is shown as a traditional paper document. However, with today's world of auditor laptop systems, this and essentially all such programs would be a library resource on the laptop system. The basic program will be constructed as

EXHIBIT 10.4 Audit Program Checklist Example: Petty Cash Example

Audit: _____ Location: _____ Date: _____

Audit step	Initial and Date	W/P Reference
1. Prior to review, determine who is the cashier responsible for the petty cash fund, the authorized fund balances, receipt requirements, replenishment procedures, and guidelines for authorized disbursements.		
2. Perform the petty cash review on a "surprise" basis. Identify yourself to the cashier, ask that the cashier function be closed during your initial review, and make a detailed count of the cash in the account as well as any personal checks included. Perform this count in the presence of the cashier and ask the cashier to acknowledge your results.		
3. If personal checks were included and if they are over one day old, ask why they were not deposited on a prompt basis. If the fund is being used as an employee short-term loan fund, with checks held as collateral, assess the propriety of this practice.		
4. Reconcile the cash count with the fund's disbursement register, noting any differences.		
5. Determine that all disbursements recorded have been made to valid employees for authorized purposes.		
6. Observe office security procedures covering the fund. Determine that the funds are locked or otherwise secured.		
7. Review procedures for fund replenishments. Select a prior period, review supporting documentation, and reconcile to purchases journal.		
8. Assess the overall control procedures, propriety, and efficiency of the petty cash process.		
9. Determine that the function is used only for authorized small cash disbursements rather than as a change or short-term loan fund.		
10. Document the results of the review and initiate corrective actions if any problems were encountered during the review.		

a secure form, such that an internal auditor can use these steps to perform a review but does not have the authority to make changes to the documented procedures. The exhibit's checklist audit program was once internal audit's most common format. The auditor would be given an audit program composed of a long list of questions requiring yes, no, or not applicable responses and would complete these program steps either through document examinations or interviews.

This checklist-format audit program has two weaknesses, however. First, while a series of auditee yes-or-no–type interview responses can lead an experienced auditor to look at problem areas or to ask other questions, these same points may be missed when a less experienced auditor is just completing the questionnaire and not going beyond the yeses and nos to see where they might lead. A procedures-oriented audit program better encourages follow-up inquiries in other areas where information gathered may raise questions.

This questionnaire-format audit program also tends to cause auditors to overlook necessary evidential matter. Inexperienced auditors can too easily check yes on the questionnaire without determining, for example, whether that response is properly supported by audit evidence. Consider a question regarding whether some critical document is regularly approved. It is easy to ask the question, receive an answer of yes, and never follow up to see if those documents actually were approved. Each of these audit program formats will work for different types of reviews *provided* the internal auditor gives some thought to the program questions. The key concern is that all audits should be supported by some type of audit program that documents the review steps performed. This approach allows audit management to recognize what procedures the auditors did or did not perform in a given review. Strong and consistent audit programs are an important step to improving the overall quality of the internal audits performed.

Going beyond the questionnaire format program, Exhibit 10.5 represents a typical, more general internal audit program format. This program describes steps in a review of business ethics processes. For each internal audit, the tasks are broken into numbered steps with space allowed for the initial and date of the internal auditor completing the audit step as well as a column for a reference to the workpaper that describes the audit step. The audit team visiting an enterprise unit could

EXHIBIT 10.5 Audit Program Format: Review of Business Ethics Procedures

Internal Control Concern	Yes	No	N/A
1. Does the enterprise have a written code of business ethics and business conduct?			
2. Is the code distributed to all employees?			
3. Are new employees given an orientation to the code of business conduct?			
4. Does the code assign responsibility to operating personnel and other stakeholders for compliance with the code?			
5. Are all employees required to acknowledge that they have read, understood, and agree to abide by the code?			
6. Are training programs delivered to all employees regarding compliance with the code?			
7. Does the code address standards that govern employee conduct in their dealings with suppliers and customers?			
8. Is there an effective mechanism in place to follow-up on reports of suspected violations of the code?			
9. Is there an effective mechanism in place to allow employees to confidentially report suspected violations of the code?			
10. Is there an appropriate mechanism to allow employees to find out the results of their reported ethics concerns?			
11. Is compliance with the code's provisions a standard used for measuring employee performance at all levels?			
12. Is there a procedure in place to update the code on a periodic basis?			

then use such standard programs to review business ethics internal controls in a consistent manner from one unit to the next. This is particularly important in a multi-unit organization where audit management wants assurance that controls over the area were reviewed and evaluated consistently, no matter who the assigned auditor or the location. This sample audit program is shown as a printed document that typically would be developed and controlled by internal audit. In other instances, the in-charge auditor might prepare a custom program to evaluate certain special procedures encountered during the field survey.

An audit program with detailed instructions or procedures assumes that the auditor using it lacks some of the technical knowledge necessary to perform the review. Such programs often are developed for one-time reviews of fairly specialized areas and prepared by audit management or a knowledgeable audit specialist with adequate knowledge to plan all of the required audit procedures. This step-by-step format is useful when a centralized audit management group with remote auditors in the field wishes to have all field auditors perform the same audit procedures.

There is no best or set format for an audit program; however, the program should be a document that auditors can use to guide their efforts as well as to record activities. This audit program will then be included in the workpapers to serve as almost a table of contents of the audit activities described in those papers. Word-processing packages and other related software can be used to prepare audit programs.

(b) Types of Program Audit Evidence

As discussed in Chapter 8, Institute of Internal Auditors standards state that an internal auditor should examine and evaluate information on all matters related to the planned audit objective. The internal auditor should gather audit evidence in support of the evaluation, what internal audit standards call *sufficient, competent, relevant,* and *useful*. An audit program, properly constructed, should guide the auditor in this evidence-gathering process. An internal auditor will encounter multiple types of evidence that can be useful in developing audit conclusions. Actually observing an action or obtaining an independent confirmation is one of the strongest forms of evidence. An auditee's often-casual response to an auditor's question covering the same area will be the weakest for of evidence. It is not that an auditor thinks the person is not telling the truth; actually observing some event is far superior to just hearing about it. Internal auditors will encounter different levels of audit evidence and should attempt to design their audit procedures to look for and rely on the best available audit evidence. Exhibit 10.6 provides some ranges of best evidence for different classifications of materials.

EXHIBIT 10.6 Internal Audit Best Evidence Classifications

Evidence Classification	Strongest	Weakest
Audit technique	Observations/confirmation	Inquiry
Origin of evidence	Corroborative materials	Underlying statistics
Relationship to auditee	External department	Internal group
Form of evidence	Written/secure system	Oral
Sophistication of evidence	Formal/documented	Informal
Location of evidence	Created in actual system	Derived or from support system
Source of audit evidence	Personal audit work	Supplied "secondhand"

The actual audit steps performed will depend on the characteristics of the entity audited. A financially oriented audit of a credit and collection function will be quite different from an operational review of a design engineering department. The financial audit might include independent confirmations of account balances; the operational audit might include extensive interviews with management and supporting documentation to assess key internal controls. Despite these differences, all internal audits should be performed and supervised following a general set of principles or standards. This will assure that internal audits are properly directed and controlled.

10.6 Audit Universe and Program Maintenance

The audit universe document is a general description of all of the audit units that an enterprise internal audit function may review. It is a plan that defines the breadth and scope of internal audit activities. To some extent, if questioned after the fact why an internal audit group has never scheduled a review in some area, internal audit can point out that the area was not included in annual internal audit plans but, more important, was never defined as part of the internal audit universe description. The universe is the big-picture map covering internal audit's territories and boundaries. It should be used as a basis for communicating with the audit committee and for planning ongoing internal audit activities.

The audit universe document is not something that should be changed on a regular basis whenever there is some small enterprise change. However, internal audit should have processes in place to keep the audit universe current and updated with perhaps regular quarterly reviews. These reviews often are good times for the CAE to explain to the audit committee any changes in internal audit's scope and operations. An effective audit universe defines internal audit annual planning and becomes a vehicle to describe an internal audit function's activities.

This chapter has introduced some formats and discussed the importance of effective audit programs. An effective internal audit function needs to establish a series of standard audit programs covering all regular audit activities. While some internal audits are done on a specialized, almost one-time basis, many others cover regular internal audit activities that may be repeated annually or even quarterly. Internal audit needs to develop a standard audit program format for all reviews as well as standard procedures for some regular, repetitive internal audits. Audit programs were once paper documents that were sometimes lost or improperly modified. Today, however, they are organized as electronic documents that are centrally controlled and located on auditor laptops. They can be a learning tool for incoming internal auditors and a mechanism by which to prepare consistent and more effective internal audits.

An understanding of how to build and use an audit universe for an internal audit function as well as supporting audit programs is a key internal audit CBOK requirement. Senior members of the internal audit team should have an overall understanding of how to build and use these tools. Internal audit staff members should understand their use and how they fit in overall internal audit processes. Perhaps even more important, internal auditors at all levels should have a strong CBOK understanding of building and using audit programs that are consistent with their audit department's established standards.

CHAPTER 11

Control Self-Assessments and Benchmarking

Much of the internal audit work described in this book discusses cases in which an internal auditor selects some area of operations and reviews the status of its internal controls. This chapter looks at two aspects of internal audit reviews and internal control assessments: control self-assessments (CSAs) and benchmarking. These are each valuable and important common body of knowledge (CBOK) internal audit procedures.

CSAs are internal audit–led processes for ongoing internal controls improvements. Rather than internal auditors visiting an area of operations and performing a formal internal audit review, in a CSA, internal audit works with local team members in some area of enterprise operations, leading them in an effort to evaluate their current control procedures and then to use the review results to improve internal controls. To many, this process is less confrontational than a formal internal audit. It can be an effective way to continue to improve internal controls in an enterprise.

In recent years, the Institute of Internal Auditors (IIA) has embraced the concept of CSA and has established formal certification examinations to recognize qualified internal auditors as leaders in this process. This chapter reviews the internal audit CSA process and describes the use of this evaluation tool for internal auditors. A high-level understanding of CSAs should be an internal auditor CBOK requirement.

Benchmarking is an internal audit technique that goes back to the IIA's progress through sharing original guidance. Back in the first days of internal auditing and when Victor Brink was launching the first editions of this book, internal auditors from different enterprises frequently met to share their approaches with peers in other businesses and to develop some best practices techniques. Benchmarking is a more formal internal audit practice of the same general nature. It is a process that allows an internal auditor to compare how similar organizations are attempting to perform and execute common practices. It often is a useful internal audit tool, and an internal auditor should have a CBOK level of knowledge on how to design and perform a successful benchmarking exercise.

11.1 Importance of Control Self-Assessments

One of the Committee of Sponsoring Organizations (COSO) internal control framework's recommendations, mentioned briefly in Chapter 3, is that enterprises "should

report on the effectiveness and efficiency of [their] system of internal control." That internal control reporting can either be at a total enterprise level or can be limited to individual enterprise departments or functions. Chapter 4 discussed internal accounting controls review from a Sarbanes-Oxley (SOx) perspective, and other chapters have covered various aspects of internal controls reviews. Several years ago and even before SOx, the IIA introduced its CSA methodology, as a process for an internal audit function to look at its own controls or for helping others to review their internal controls. Based on the total quality management approaches of the early 1990s (highlighted in Chapter 30) as well as the COSO internal controls framework discussed in Chapter 3, the CSA methodology has become a powerful tool for internal auditors and others to better understand an enterprise's internal control environment. The approach requires internal auditors to assemble a special team to assess those internal controls.

CSA was first developed in 1987 by a team of internal auditors at Gulf Canada as a tool to assess its internal control effectiveness as well as business processes. At that time, Gulf Canada was facing both a legal consent decree requiring it to report on its internal controls as well as some difficulties resolving oil and gas measurement issues through traditional audit assessments. Gulf Canada's internal audit group launched a *facilitated meeting* self-assessment approach that involved gathering management and staff for interviews relating to, and discussions of, specific internal controls issues. The process became CSA, a mechanism to assess informal, or soft, controls as well as the more traditional hard controls, such as accounting balances.

That CSA approach was published and has been adopted by a number of major corporations and has become part of IIA *International Standards for the Professional Practice of Internal* Auditing (see Chapter 8). This chapter describes the CSA process in more detail and discusses the potential value to an enterprise in using CSA, how internal audit can launch CSA, and how to evaluate the data and results from a CSA project. CSA can be an important and useful tool for many internal audit organizations.

11.2 CSA Model

CSA is a process designed to help departments within an enterprise assess and then evaluate their internal controls. In many respects, the CSA approach uses some of the same concepts found in the COSO internal controls framework discussed in Chapter 3. The CSA model says that an enterprise must implement strong control objectives and control activities in order to have an effective control environment. These two elements are surrounded by a good system of information and communication as well as processes for risk assessments to monitor performance. This CSA model is shown in Exhibit 11.1.

CSA is a continuous improvement process similar to methods described and used by quality assurance (discussed in Chapter 31). The concept calls for a team to establish and improve their controls environment by establishing goals and objectives regarding those controls, then performing a risk assessment to better understand those designated control risks, to implement controls activities to reduce identified risks, and then to monitor the performance of these improved controls. This is a continuous process. The CSA team can start in any quadrant of the model shown in the exhibit and then move to the next phase in a clockwise manner.

EXHIBIT 11.1 CSA Process

The CSA is a controls assessment process that some professionals consider more accessible than Chapter 5's *C*ontrol *ob*jectives for *i*nformation and related *T*echnology (CobiT) internal controls model. Some business professionals, for example, look at a COSO internal controls risk assessment process as too "high level" and difficult to understand. In CSA, individual departments in an enterprise can formally meet, in a facilitated group format, and assess the risks and internal controls within their individual functions. Many internal audit departments have used CSA as a method to encourage departments to think about how to improve their internal controls.

11.3 Launching the CSA Process

CSA is a process through which internal control effectiveness is examined and assessed not by a team of outsiders, such as consultants or even internal auditors, but by people from within the function being assessed. Internal audit often takes a leadership role here. The CSA objective is to provide reasonable assurance that good internal control business objectives will be met. The CSA concept requires gathering management and staff for interviews to assess their internal controls environment—a controls self-assessment. Because CSA requires all people in a function to participate in these sessions, from senior managers to staff, it often works best when someone outside of the department acts as a facilitator. Many people can take this CSA facilitator role, but internal audit is often a key group, ideal for this role because of its internal controls review background. A separate quality audit function, as discussed in Chapter 31, often is a major help here as many of its approaches are similar to the CSA model approach.

The CSA process works particularly well when an enterprise has some business unit whose internal controls do not match exactly with the rest of other enterprise operations. For example, assume an enterprise manufactures some type of plant production equipment used by other manufacturing businesses. Also assume that there are good production and product internal controls for the overall enterprise, but because these are high-value components, customers may return these finished goods to a rework facility from time to time to upgrade them to a new version. The rework facility cleans up and upgrades the products for sale as used equipment to other markets. This type of rework facility would be an ideal candidate for a CSA review. It probably would have different but similar processes when compared to the prime manufacturing business. Because its work is specialized compared to the mainstream production business, the rework facility team members would understand both regular production and rework operations. We refer to this type of rework facility in our CSA descriptions.

Regardless of who acts a leader or facilitator, a CSA project should improve an enterprise's control environment by making involved stakeholders more aware of their specific departmental objectives and the role of internal control in achieving goals and objectives. A basic concept behind the CSA process is to motivate members of an enterprise unit to design and implement their own internal control processes and then to continually improve them. Our example of a specialized rework facility would be a good fit for this type of CSA review process. A CSA review can be particularly effective, for example, when the internal control process reviewed is a large enterprise resource planning (ERP) system that covers all or most aspects of operations. Our example rework facility uses ERP components only partially. In an ERP, one basic automated system covers accounting, human resources, production, marketing, and more. The ERP covers many aspects across an enterprise, but the members of the example rework facility may not fully understand the internal control implications of such a large, all-encompassing system and the results of their various individual actions.

As a good first step to launch CSA processes in an enterprise, the chief audit executive (CAE) or some other person leading the initiative will need to sell the CSA concept to senior management. In a smaller enterprise, the message may be that CSA should help the enterprise to improve internal control procedures and SOx Section 404 compliance while not embarking on a time-consuming, expensive exercise. Other potential benefits from such a CSA process are:

- Increasing the scope of internal control reporting during a given period
- Targeting internal control-related work by placing a greater focus on high-risk and unusual items discovered in the course of these CSA reviews
- Increasing the effectiveness of internal audit–recommended corrective actions by transferring internal controls ownership and responsibility to operating employees

Published results indicate that CSA is an effective technique for improving the internal control environment. Perhaps the worst way for an enterprise to use CSA, however, is for the CAE or some other member of internal audit management to attend an IIA-sponsored CSA seminar, come back enthused, and then work with operations management to launch a big-picture, wide-ranging comprehensive CSA program without understanding the necessary details steps to make it successful. This

is almost certainly a mistake. An enterprise should start small and launch CSA initially in a single business unit where there is a general feeling that control improvements are needed. Internal audit should explain the process to management and obtain approvals to launch CSA, at least as a pilot program. Going beyond a traditional audit review, internal audit will normally run a CSA program with one internal auditor designated as the team lead.

The CSA team leader then needs to refine the review area in more depth and decide what portion of the entity will use CSA, what functions or objectives to consider, and what level of stakeholders should be included in the assessments. The number and level of stakeholders will depend on the CSA approach selected. Three principle primary CSA approaches are *facilitated team meeting workshops, questionnaires,* and *management-produced analysis*. Internal audit–led CSA teams often combine a mixture of more than one approach to accommodate their self-assessments.

Facilitated team meetings gather internal control information from work teams that may represent multiple levels within an enterprise. A facilitator trained in internal control system design, often from internal audit, information technology (IT), or quality assurance, should lead these sessions. The questionnaire-based approach uses surveys that usually are based on simple yes/no or have/have not responses. Process owners use the survey results to assess their control structure. The third approach, a management produced analysis, is really an internal audit type of analysis. Based on a study of the business process produced by management or staff, a CSA specialist—probably an internal auditor—combines the results of the study with information gathered from sources such as interviews with other managers and key personnel. By synthesizing this material, the CSA specialist develops an analysis that process owners can use to better understand and improve internal controls for the given process area.

The CSA approach and format used depends on the overall organizational culture as well as senior management decisions. In the event a corporate culture does not support a participative CSA approach, questionnaire responses and internal control analysis can enhance the control environment. The facilitated session works the best where all employees meet on a peer basis and discuss and evaluate their internal control issues and concerns in open, facilitator-led discussions.

Just as there was some discussion (see Chapter 4) on the role of internal audit in early days of SOx Section 404 reviews, the same issues may be raised for CSA processes. There must be a decision as to what department will drive the CSA process: internal audit or operating management. Some CSA practitioners believe that internal audit, as the arm of senior management responsible for internal control oversight, may be the appropriate driver for CSA. The presence of internal auditors in CSA-facilitated meetings is, in and of itself, an oversight control. Others believe that a self-assessment can be performed effectively only by operating management and/or work units. The involvement of internal audit, in this view, means that management will be less accountable for internal controls. Internal auditors, in their roles as enterprise internal consultants, are very qualified to lead such efforts.

(a) Performing the Facilitated CSA Review

The basic concept behind a CSA review of an internal control system or process is to gather a group of people, across multiple levels of the enterprise and from

multiple units, and then collectively gather extensive information from that group about the internal controls for that selected system or process. The idea is to have a representative sample of stakeholders throughout the enterprise meet and discuss these designated enterprise operations and controls. Our example of a rework facility in a manufacturing operation would be a good fit here. An internal auditor or some other communications specialist would be designated to head these workshops, lead discussions, and help draw conclusions.

Facilitated workshops gather information from teams representing different levels in the business unit or function. The format of the workshop may be based on objectives, risks, controls, or processes. Each has distinct advantages depending on the internal controls area reviewed. Assume, as an example, that an enterprise has installed a large, comprehensive ERP system that encompasses many major operations areas. Management has requested an internal control risk assessment of this major application. Because the ERP system covers many aspects of business operations, a decision is made to review systems controls through a series of focus group users gathering to discuss and review systems operations. Steps for organizing these reviews should be developed into a CSA enterprise plan. Based on the extensive set of CSA materials published by the IIA,[1] this plan and a facilitated CSA session should follow any of four meeting formats:

1. **Objective-based CSA facilitated sessions.** These sessions focus on the best way to accomplish a business objective, such as accurate financial reporting. The workshop begins by the team identifying the controls currently in place to support the system objectives and then determining any residual risks remaining if these controls are not working. The aim of this workshop format is to decide whether the control procedures are working effectively and whether any remaining risks are within an acceptable level. This type of facilitated session could begin by the facilitator asking participants to identify their group's control environment, emphasizing such areas in the control environment as:
   - The control consciousness of the enterprise
   - The extent to which employees are committed to doing what is right or doing it the right way
   - A wide variety of factors encompassing technical competence and ethical commitment
   - Intangible factors that are often essential to effective internal control
2. **Risk-based CSA facilitated sessions.** These sessions focus on the CSA teams listing risks to achieve internal control objectives. The workshop begins by listing all possible barriers, obstacles, threats, and exposures that might prevent achieving an objective and then examining the control procedures to determine if they are sufficient to manage any identified key risks. The aim of the workshop is to determine significant residual risks. This format takes the work team through the entire set of objective-risks-controls surrounding the entity reviewed. This would follow with risk-based discussions. Teams would be asked to identify their risks by asking themselves such questions as:
   - What could go wrong?
   - What assets do we need to protect?
   - How could someone steal from us?
   - What is our greatest legal exposure in this area?

Sessions would attempt to identify significant risks at department, activity, or process levels. For each identified risk, the groups should discuss the potential likelihood of occurrence and the potential impact. Those risks with a reasonable likelihood of occurrence and a large potential impact would be identified as significant.

3. **Control-based CSA facilitated sessions.** These sessions focus on how well the controls in place are working. This format is different from the last two sessions because the facilitator identifies the key risks and controls before the beginning of the workshop. During this type of CSA session, the work team assesses how well the controls mitigate risks and promote the achievement of objectives. The aim of the workshop is to produce an analysis of the gap between how controls are working and how well management expects those controls to work.
4. **Process-based CSA facilitated sessions.** These sessions focus on selected activities that are elements of a chain of processes. Processes are a series of related activities that go from some beginning point to an end, such as the various steps necessary in either purchasing, product development, or revenue generation. This type of workshop usually covers the identification of the objectives for the selected process and its various intermediate steps. The aim of this type of workshop is to evaluate, update, validate, improve, and even streamline the whole process and its component activities. This type of session format generally requires a greater breadth of analysis than just a control-based approach. Facilitated sessions here cover multiple objectives within the process and support concurrent management efforts, such as reengineering, quality improvement, and continuous improvement initiatives.

Each of these formats can be effective for developing and understanding both hard and soft controls[2] in a function as well as the risks surrounding any significant internal control processes. The keys to success here are to have knowledgeable and well-prepared meeting facilitators ask appropriate questions and get all team members to participate. A major requirement for any CSA session is to take detailed transcriptions of the meeting sessions. While not every word spoken has to be recorded, strong meeting note summaries are needed. Recording major discussion points on a large pad in front of the room often works well.

While the facilitator is a major driver here, CSA sessions can easily turn into disasters with the wrong people mix. Lower-level stakeholders may feel reluctant to discuss controls weaknesses if people who are more senior are also attending the session. Comments about risks or control weaknesses can get very personal if some team members have major responsibilities for the systems or process discussed. Despite all of this, the CSA process can be a very worthwhile but expensive tool to look at a comprehensive system or process from multiple perspectives and to understand any internal control weaknesses.

(b) Performing the Questionnaire-Based CSA Review

A CSA-facilitated review can be difficult and time consuming, no matter whether it is relative risk, internal control, or process based. In many cases, a questionnaire can be an effective way to gather internal control information. A questionnaire can be prepared covering the process or system and then distributed to a select group

EXHIBIT 11.2 CSA Specific Function Questionnaire: Planning and Budgeting

These questions might be used for a Planning and Budgeting CSA review:

1. Do you ensure that completed budgets are consistent with the strategic plan of the company?
2. Are policies and procedures in place to avoid understatement of expenditures?
3. Do you investigate all variances between actual expenditures and budgeted amounts, and, for all variances, are explanations required?
4. Do you ensure that the finalized budget and all approved revisions are properly documented and approved?
5. Have you assigned a person to receive all information regarding changes to the company that may affect the budget?
6. Is the budget preparation procedure (including approval-level requirements) fully documented, and is it distributed to all management involved in the budget process?
7. Are procedures in place to provide adequate information to departmental management for their use in developing a budget?
8. Do you monitor both short- and longer-term trends in expenses?
9. Are the calculation methods for expenses (including new categories) adequately explained?
10. Do you ensure that departments are given adequate time to complete and submit their budgets?
11. Have you identified one individual within each department who has the responsibility for completing the budget, and is assistance provided as needed?
12. Do you advise departments on what and how expenses are to be charged for acquisitions or disposed operations?
13. Are procedures in place to ensure that a limited number of authorized indiviuals have access to the budgets and that any additions, changes, and deletions are approved and traceable? If the budget is online, are all transactions identified by userid, date, and transaction type?
14. Do you review the initial budgets and identify areas of possible cost reductions?
15. Are procedures in place to identify departments that consistently incur large expenditures at year-end to bring actual costs up to budget?
16. Are procedures in place to handle cash forecasts?
17. Do you monitor and require approvals for all capital expenditures?
18. Have you identified all of the documentation required of departments when submitting numbers for budgets, return on investments calculation, etc.?
19. Do you monitor project breakdown to ensure that large projects are not broken down into smaller projects to avoid approval requirements?

of stakeholders to gain an understanding of the risks and controls in the area of interest. Exhibit 11.2 is an example CSA questionnaire for planning and budgeting processes. It was developed from IIA materials. The IIA has an extensive set of sample CSA questionnaires on its Web site: www.theiia.org.

The CSA team would circulate these questionnaires, with the respondent's name attached, to a selected group of stakeholders, monitor results to assure that an appropriate number have been returned, and then compile the results. Questionnaires will not yield the discovery-type comments that come out of focus groups but will give an overall assessment of the soundness of processes and internal controls. This is an effective way to gather basic CSA background data.

(c) Performing the Management-Produced Analysis CSA Review

As an alternative to a survey or a facilitated workshop, a management-produced analysis is very similar to the type of operational review that an internal auditor would perform. This is one of the three CSA analysis approaches suggested by the IIA. Using this approach, management produces a staff study of the business process—almost a research study. The CSA specialist, who may be an internal auditor, combines the results of the study with information gathered from other sources, such as managers and key personnel. By synthesizing this material, the CSA specialist develops an analysis that process owners can use in their CSA efforts.

The management-produced CSA analysis approach, although endorsed by the IIA, is difficult for the typical enterprise. It suggests an almost "academic" review by someone in the enterprise followed by some comparative research for subsequent analysis. We generally do not recommend this IIA-endorsed alternative approach.

The IIA believes all of the three formats strengthen the entity's control structure. Each entity should analyze external opportunities and threats as well as internal strengths and weaknesses to determine which format is most appropriate to use. Many CSA users combine one or more formats within a given facilitated meeting to best meet their needs.

11.4 Evaluating CSA Results

A CSA analysis, particularly if it covers multiple processes or systems, will result in a large amount of data. Some may support existing process strengths, others will point to internal control weaknesses in need of correction, and still others may point to areas in need of further research. In most cases, however, the CSA review work will validate the integrity and controls of the systems and processes reviewed.

The results of this CSA review will be similar to a COSO review of internal accounting controls—a disciplined and thorough method to evaluate significant internal controls. This can also be a good first step to launch a SOx Section 404 analysis, as described in Chapter 4. CSA provides a way for reviewers to gain a better understanding of the many hard and soft controls that surround many processes or systems. Published documentation or focused controls review interviews may indicate that some controls exist. However, the back-and-forth from a facilitated session may reveal that "Yes, there are control processes described in our systems documentation, but we always push the escape key to ignore the control warning messages." This type of CSA session discussion information can be an effective way to expose internal control vulnerabilities.

CSAs were introduced to the internal audit community in the late 1980s and were embraced by the IIA. Many private-sector enterprises worldwide initiated successful CSA programs, and several state governments within the United States now require CSA-oriented internal control assessments. The auditing and accounting departments within those states complied with the CSA requirements via questionnaires or management-produced analysis processes. The Federal Deposit Insurance Corporation (FDIC) and the Canadian Deposit Insurance Corporation (CDIC), for example, each now require financial institutions throughout the United States and Canada, respectively, to assess internal controls with specific CSA guidance compliance.

To support the CSA process, the IIA has launched a specialty certification, the Certification in Control Self-Assessment (CCSA). This examination-based certificate is designed to enhance senior management's confidence of a reviewer's understanding, knowledge, and training of the CSA process. The CCSA certificate and its requirements, as well as other internal auditing professional certifications, are discussed in Chapter 27.

The IIA believes that CSA processes effectively augment the profession of internal auditing. One of the primary responsibilities of the board and officers of any enterprise is providing stakeholder assurance through oversight of the enterprise's activities. Internal auditing, by definition, assists members of the enterprise in the effective discharge of their responsibilities. Through CSA, internal auditing and operating staff can collaborate to produce an assessment of internal controls in an operation. This synergy helps internal auditing assist in management's oversight function by improving the quantity and quality of available information. The quantity is increased as internal auditing relies on operating employees to actively participate in CSA reviews, thus reducing time spent in information gathering and validation procedures performed during an audit. The quality is increased because participating employees have a more thorough understanding of the process than an internal auditor can develop over a relatively short time. As we discussed in the introduction to this chapter, a basic knowledge of how to organize and conduct a CSA process should be part of an internal auditor's CBOK.

11.5 Benchmarking and Internal Audit

Benchmarking is one of those professional terms that is frequently used but often misused. That is, it is often easy for a professional to say "We benchmarked that process" when an internal auditor asks some process-related questions. However, if that same internal auditor asks to see the results of the benchmarking study, no formal documentation may be available to support the analysis.

Benchmarking is a "best practices" process where an enterprise evaluates various aspects of its processes in relation to best practices, usually as performed within other peer enterprises. After such an analysis and comparison, an enterprise can develop plans on how to adopt these other best practices, usually with the aim of increasing some aspect of performance. Benchmarking sometimes is a one-time event, but it is often better treated as a continuous process in which an enterprise continually seeks to challenge and improve their practices. In simple terms, it is a process where an organization compares its processes with other, better (it is hoped) processes to improve process standards and to improve the overall quality of a system, product, or process.

Benchmarking is a powerful management tool because it overcomes what some consultants call "paradigm blindness." In this mode of thinking, management believes that the way the enterprise does things is best because that is the way things have always been done. Benchmarking can open an enterprise to new methods, ideas, and tools to improve its effectiveness. It helps crack through resistance to change by demonstrating other methods of solving problems from the one currently employed and by showing that they work, because they are being used by others.

Benchmarking approaches are important to internal auditors from two perspectives. First, the use of benchmarking can be very powerful internal audit

recommendation when reviewing operations in some area. An internal auditor often sees obvious internal control weaknesses but may not have enough knowledge in an area to make comprehensive internal control improvement recommendations. A strong recommendation, however, would be for internal audit to recommend that some operating unit use benchmarking studies to achieve best practices in some area. We discuss how to launch and implement in the next section.

Internal auditors also need benchmarking to improve their own internal audit practices. The IIA has promoted the concept of "Progress through Sharing" to improve the practice of internal auditing since its founding in the late 1940s. Many ideas were shared through presentations and informal discussions at IIA chapter meetings, but the IIA is worldwide today, with many seeking to share these data and the Internet available to facilitate that sharing. The IIA has launched the Global Audit Information Network (GAIN) to share best ideas and promote internal audit best practices. Later in the chapter we briefly review GAIN and how it is promoting internal audit best practices.

(a) Implementing Benchmarking to Improve Processes

There are no accepted standard professional procedures for launching a benchmarking process. Therefore, many variations exist regarding what professionals call benchmarking. However, benchmarking should be a process that allows an enterprise unit to compare how it is performing against its peers in some area of operations. To better describe how benchmarking works, we focus on a benchmarking effort that this author led for a larger corporation in the mid-1990s.

For background, this author had a lead role in launching business compliance and ethics function for a large, Chicago-area corporation. This was a new initiative for that enterprise, and at that time, not many other major corporations had similar functions. This process was essentially a service-type function with no fears of giving out trade secrets. An enterprise manufacturing a patented consumer shampoo product, for example, cannot visit a series of competitors to see how they are manufacturing a similar product. Too many confidentiality trade issues arise. However, many other enterprises are freely—and sometimes proudly—willing to share how they are performing in some area. The next steps describe how this author launched a successful benchmarking study some years ago. The necessary steps to launch benchmarking are described from the perspective of this author's project. The author's actions are described using the word *we,* but these actions should apply to internal auditors acting as internal consultants and the team launching a benchmarking study.

1. **Defin the objectives of the benchmarking study.** It sounds almost obvious, but a first step is to define what an internal auditor wants to learn from the benchmarking exercise. In this example, we wanted to launch an ethics "help desk/hotline" function where employees could anonymously call in observed code of conduct violations and also ask ethics and code of conduct questions. We were aware that some other corporations were doing this and wanted to develop an improved or best practices process.
2. **Establish a set of potential benchmark partners who were willing to participate.** In this case, we were aware through professional meetings and publications of other companies that were doing something similar. This is an

important benchmarking planning step. Too many partners can be difficult to manage, but too few may not give much representative information. Names and contacts can be gathered through professional meetings and conferences.

3. **Develop specifi goals and objectives for the benchmark study—what do we want to learn?** This step defines what we want to learn from our study. Since time and logistics typically prevent direct visits, much of our information must come from responses to questionnaires, with telephone follow-ups. Benchmarking surveys usually are designed to allow another enterprise to brag about some best practice. They are not exercises where outsiders typically talk about their problems or what did not work.
4. **Clear up legal and confidentialit issues.** In any benchmarking study, the reviewers will be asking other enterprises to disclose some potentially confidential company information. By asking these questions, we sometimes are admitting that we may have deficits in the area we are reviewing. The process should be reviewed with enterprise legal resources to avoid any pitfalls. The benchmarking study will need to have some strong declarations out front that strongly state that any data gathered will be kept strictly confidential.
5. **Contact potential benchmarking partners.** After all of the preliminary work, we should contact potential participants for the study. This often works best when professional personal contacts may have been established. The proposed benchmarking project should be outlined with these objectives:
   a. The purpose of our benchmarking study—what are we trying to learn?
   b. Why have we selected this potential participant?
   c. What specific information are we seeking, how will we gather it (e.g., questionnaire), and how much time will it take?
   d. Strong statements on confidentiality—we will not reveal or compromise any company information.
   e. An offer to give something as a result of participation. This is usually the promise to share the total results of the study with all participants.
   f. A request for an acknowledgment that they will be willing to participate.
6. **Gather benchmarking information.** In this step, we gather our benchmarking data from each participant. While benchmarking study participants usually require the sending out of fairly detailed questionnaires, telephone calls or even site visits are possibilities. The idea is to find out as much as we can what our participants are doing in our area of interest.
7. **Gather and scrub results.** After we have completed our benchmarking surveys—care should be taken not to drag things out over too long of a time period—the survey information should be assembled and reviewed to answer our questions. Any potentially confidential information gathered regarding other company names and identities should be scrubbed or removed.
8. **Publish benchmarking results and make changes, as appropriate.** The whole purpose of any benchmarking study is to see what others are doing as best practices in an area of interest. In the author's study, we found we were doing a superior job in the area of interest, and there were only a few recommendations to be gained from the study.

We have described a benchmarking study in very general terms. Benchmarking is often a very good way to gather best practices information from other enterprises.

Professionals from other enterprises are often very willing to brag about their own operations and how well they are doing some business practice.

Internal auditors can launch benchmarking studies as a way to see how other internal audit functions are approaching some practice or approach. Benchmarking here should go a little beyond casual conversations about internal audit practices with other internal audit peers as part of an IIA chapter meeting. An internal audit function may elect to launch a benchmarking study about some best practice technique with other internal audit chapters, even on a worldwide basis. Internal audit's sharing processes will encourage this, and a formal benchmarking study will add some support to the results.

An internal auditor acting as an enterprise consultant, as discussed in Chapter 28, is often an excellent resource to help an enterprise in implementing benchmarking. During audits, internal auditors often suggest that some business unit improve its processes through benchmarking. As discussed, all too often *benchmarking* is a term that is used carelessly. Internal auditors with an understanding of the benchmarking process can engage in a separate internal consulting project to help their auditees establish effective benchmarking procedures.

(b) Benchmarking and the IIA's GAIN Initiative

As discussed, the IIA was an early proponent of benchmarking approaches through its "Progress through Sharing" motto. The IIA decided to formalize things through its GAIN benchmarking forum. First established by the IIA in 1992, GAIN did not receive a large amount of attention in its early years. However, recently the GAIN initiative has been better formalized. The IIA's GAIN is a knowledge exchange forum to:

- Share, compare, and validate internal audit practices
- Network with other internal audit functions
- Learn from the challenges and solutions of internal audit peers
- Enhance leading internal audit practices from top organizations
- Enhance internal audit operational effectiveness and efficiency

As a separate IIA initiative, IIA's GAIN publishes extensive and comprehensive benchmarking studies regarding global internal audit activities. The IIA GAIN program asks its member internal audit functions to register and to complete a fairly detailed questionnaire about their internal audit function. Exhibit 11.3 is an extract from this questionnaire. The IIA's GAIN function is attempting to gather information about each cooperating internal audit function.

Upon completion of an internal audit function's questionnaire, the response data is validated and added to the GAIN Annual Benchmarking Study database. From an internal function's questionnaire answers, a variety of unique GAIN internal audit benchmarking reports are available that can reflect the activities of an internal audit function in contrast to its peers. While a wide variety of customized reports are available specific to industry groups and other attributes, GAIN publishes an annual internal audit benchmarking report that shows an internal audit function how it is doing compared to peer internal functions. These annual reports are available for purchase through the IIA. Exhibit 11.4 is a sample GAIN annual benchmarking survey table of contents. GAIN gathers contributed data from worldwide internal audit functions. There is a lot of valuable data here, and CAEs should use these

EXHIBIT 11.3 IIA GAIN Annual Benchmarking Questionnaire Example

This exhibit, extracted from several sections of the much larger comprehensive GAIN survey questionnaire, lists the types of information that the IIA is requesting its GAIN participants to submit about their internal audit function. This information is then combined with other submissions to form annual internal audit benchmarking studies. These topics, selected from the IIA's GAIN Web site, show the types of benchmarking information that the IIA is attempting to collect.

Section A: Enterprise Information

- Revenues, assets, and expenses as of and for the most recent fiscal year-end from the enterprise's financial statements.
- Total full-time personnel equivalents for the enterprise.

Section B: Internal Audit Resources

- Total costs of internal audit activities categorized as follows:
  - Salary (gross pay and bonuses)
  - Employee benefits (if not tracked separately, averages 30% of salaries)
  - Travel and training
  - Costs of sourced services (e.g., consultants, co-source providers, etc.)
- Total internal audit staff differentiating between in-house staff versus sourced staff using the following categories:
  - Chief Audit Executive
  - Directors and managers
  - Seniors and supervisors
  - Staff
  - Secretarial and clerical

  For each staff level outlined (excluding clerical), provide information regarding the level of education sought, average years in internal audit profession, average years in enterprise's primary industry, and the number of staff at each level with one or more professional designations (certifications).

. . .

Section D: Risk Assessment and Audit Planning

- Number of auditable activities or units in audit universe (all possible audits planned and actual audits for year).
- Components of audit plan categorized by assurance engagements, consulting engagements, management requests, fraud investigations, and follow-up audits.
- Percentage of management requests that were actually accomplished.
- Information on type and creation of audit plans.
- Information on type and creation of enterprise/internal audit risk assessments.
- Number of risk categories used and percentage coverage of those categories by the audit plan, if applicable.
- Information on type and creation of engagement-level audit plans.

Section E: Audit Implementation/Life Cycles/Reporting

- Total audit staff time categorized as follows:
  - Assurance engagements
  - Consulting engagements
  - Fraud investigations
  - Management requests
  - Follow-up audits
  - External audit assistance
  - Nonchargeable time—training and other
  - Absences
- Percentage of audit time spent on planning, fieldwork, and reporting.
- Calendar days (business days) to complete: planning, fieldwork, reporting, and follow-up.
- Calendar days that lapse between the end of fieldwork and the issuance of draft reports and the end of fieldwork and the issuance of final reports.
- Number of audit recommendations, major audit findings, and repeat findings identified during the year.
- Percentage of recommendations actually implemented.

Source: www.theiia.org.

EXHIBIT 11.4 GAIN Annual Benchmarking Survey Table of Contents

Section 1: Demographic Information
Demographic Information: Financial
Respondents by Expense Class
Demographic Information: Employees
Respondents by Industry
Organizational Demographics
Sarbanes-Oxley Status
Section 2: Summary Information
Revenues and Assets per Auditor
Expenses and Employees per Auditor
Section 3: Internal Audit Costs
Summary of Audit Costs
Salary and Benefits as a Percentage of Total Audit Costs
Travel and Training as a Percentage of Total Audit Costs
Total Costs per Auditor (with and without Travel)
Travel and Training Costs per Auditor
Section 4: Internal Audit Staffin
Internal Audit Staff Profile
Change in Internal Audit Staff Size
Summary of Professional Audit Staff by Function
General and IT Auditors as a Percentage of Total Auditors
Fraud and ESH Auditors as a Percentage of Total Auditors
Level of Education Sought for Auditors
Internal Audit Experience of Auditors
Industry Experience of Auditors
Number of Staff with Professional Designations
Percentage Staff with Professional Designations
Professional Designation Mix
Level of CIA Designation Required
Internal Audit Hiring Practices
Staff Turnover
Section 5: Sourcing
Sourced Staff Profile
Costs of Purchased Services
Level of Sourcing
Audit Activities Sourced
Sourced Hours and Fees
Fees for Purchased Services
Future Reliance on Sourcing
Section 6: External Audit
External Audit
Internal Audit Assistance on External Audit
External Audit Fees as Percentage of Total Revenues, Assets, and Expenses
Section 7: Internal Audit Oversight
IA Oversight and Areas of Focus
Section 7.1: Internal Audit Oversight—Chief Audit Executive
CAE Reporting Line
Title of Chief Audit Executive
Responsibilities of Chief Audit Executive
Section 7.2: Internal Audit Oversight—Audit Committee
Audit Committee
Audit Committee Chair

Source: www.theiia.org. (*Continued*)

EXHIBIT 11.4 GAIN Annual Benchmarking Survey Table of Contents (*Continued*)

Audit Committee Meetings
Presence of Audit Committee Charter
Responsibilities of Audit Committee
Information Shared with Audit Committee
Professional Development of Audit Committee Provided by Internal Audit
Evaluations of Audit Committee and Charter

Section 8: Risk Assessment and Audit Planning

Section 8.1: Audit Universe
Audit Universe
Audit Performance
Percent of Audits Planned Actually Performed
Percent of Audit Universe Audited
Audits per Auditor
How Audit Universe Is Determined

Section 8.2: Audit Plan
Allocation of Audit Plan
Percent of Management Requests Completed
Type of Audit Plan
Years Covered by Audit Plan
How Audit Plan is Created

Section 8.3: Risk Assessments
Presence of Formal Risk Assessment
Process for Internal Audit
Frequency of Internal Audit Risk Assessment
Factors Influencing Risk Assessment
Risk Assessment Rating Criteria
Risk Categories
Percentage of Risk Categories Covered by Audit Plan
Presence of Engagement Level Risk Assessments
Engagement-Level Risk Assessments—Information Gathering
Engagement-Level Risk Assessments

Section 9: Audit Implementation/Life Cycles/Reporting
Allocation of Audit Staff Time
Audit Life Cycle
Audit Life Cycle—Reporting
Tools and Techniques Utilized on Audits.
Audit Engagement Reporting

Section 9.1: Observations and Follow-up Audits
Expressing an Opinion on Internal Control
Audit Follow-Up Activities
Presence of Audit Recommendations
Audit Recommendations
Major Audit Findings Identified
Major Audit Findings—Metrics
Repeat Findings
Percent of Recommendations Actually Implemented

Section 9.2: Continuous Auditing
Continuous Auditing
Responsibility of Continuous Auditing
Continuous Auditing Operations
Benefits and Obstacles of Continuous Auditing

Section 10: IT Auditing
IT Audit Group
Integration of IT and General Audits

data to better understand how their internal audit function is doing compared to others. One area that is surprising, however, is the lack of benchmarking data gathered regarding IT audit issues and practices. GAIN does not appear to be giving enough benchmarking attention to that very important area.

The IIA's GAIN function also does a wide variety of what it calls Flash Surveys. For example, it polls participating internal audit groups and asks, for example, if they use automated or manual tools to develop and product their internal audit reports. These surveys are generally limited to some 300 to 400 responses and provide some basic yes/no responses. While one can argue about the depth and auditor understanding of some of these responses, often these surveys provide good background information to allow a CAE to assess what other internal audit functions are doing.

The IIA GAIN function has come a long way in allowing internal auditors to better understand what their peers are doing as part of their internal audit practices. The responses to the GAIN questionnaires are only as good or accurate as the internal audit function-by-function data entered. However, these GAIN data provide an overview of many of the practices that are important to all internal auditors. CAEs should strongly consider enrolling in the GAIN benchmarking surveys and studies to understand areas that other internal auditors are emphasizing. Doing so greatly improves the sharing of information among internal auditors.

11.6 Better Understanding Internal Audit Activities

This chapter has introduced two important internal auditor tools: control self-assessments and benchmarking. CSAs say that rather than internal auditors performing formal review in some areas, internal audit often can provide overall value to all parties by promoting a control self-assessment. While not appropriate in some areas, this approach encourages internal auditors to act as internal consultants and to lead efforts with their own enterprise to encourage front-line teams to look at their own internal controls and to implement improvements. This can be a very effective tool on many levels, and internal auditors should have a CBOK understating of how to launch controls assessment processes.

An understanding of benchmarking is an even more important internal auditor CBOK requirement. As discussed, benchmarking is one of those terms that are used too often without a complete understanding of the process. Internal auditors should have a basic CBOK understanding of the benchmarking process, whether they use it to gain best practice information from other internal audit functions or to serve as an enterprise consultant to help enterprise personnel launch their own benchmarking studies.

Notes

1. Institute of Internal Auditors Research Foundation, *Control Self-Assessment: Experience, Current Thinking, and Best Practices* (Altamonte Springs, FL: 1996).
2. *Hard controls* refer to controls built into IT or other formal systems, while *soft controls* are based on either published procedures or stakeholder recognition that they are the rules.

PART IV

Organizing and Managing Internal Auditor Activities

CHAPTER 12

Internal Audit Charters and Building the Internal Audit Function

This chapter and the other chapters in Part Four cover the essential activities of an internal audit department, from launching the function in this chapter to reporting internal audit results in Chapter 17. This chapter introduces some of the practices necessary to build an effective internal audit function, starting with an authorizing charter and the basic processes of building, staffing, and managing an effective internal audit department. We begin by describing the need to establish a formal internal audit charter, a basic authorizing document that has some common elements no matter whether internal audit is serving a large multinational corporate structure or a smaller not-for-profit entity. This is the document approved by the audit committee that outlines internal audit's authority and responsibility to operate within an enterprise.

The chapter discusses steps to building an effective internal audit function, including typical internal audit position descriptions and organization structures. An internal audit function will base many of its efforts on defining and understanding its audit universe (the number of potential auditable entities in the enterprise), as was discussed in Chapter 10. No matter what industry, geographic location, or size of the enterprise, all internal audit departments or functions need to follow some similar good practice procedures.

Most of this book's common book of knowledge (CBOK) theme covers technical internal audit areas, such as information technology (IT) application control reviews or guidance for assessing the results of audit evidence. This chapter and the others in Part Four discuss steps for launching and managing an effective internal audit function. When Victor Brink launched the first edition of this book shortly after World War II, many enterprises had heard of the potential benefits of internal auditing and wanted to learn more about how to establish such a function in their own enterprise. The first edition of *Brink's Modern Internal Auditing* helped to launch the internal auditing profession, but today's world of professional internal auditing is much more complex. While there still are start-up enterprises that do not have an internal audit function, many enterprises in North America, the European Union countries, and major nations in Asia have established internal audit functions.

This chapter reviews the steps necessary to start an effective internal audit function, including the importance of a formal charter authorized by the audit committee and building an effective internal audit staff. We also review important internal audit policies and procedures as well as the first steps to review enterprise-auditable entities. This material should help a new, start-up enterprise launch an internal audit function that follows some recommended best practices.

12.1 Establishing an Internal Audit Function

There is no one optimal way to organize an internal audit function in an enterprise today. There can be many differences in type of business, geographic span, and organization structure, with differing internal audit needs for each. Each, however, must follow the *International Standards for the Professional Practice of Internal Auditing*, as discussed in Chapter 8, but should have the support and recognition of enterprise management. The need to have an internal audit function generally comes from legal requirements, such as the Sarbanes-Oxley (SOx) Act, or other requirements from governmental agencies. When an entity does not have an internal audit function, senior management should take steps to launch such a function.

The head of an internal audit function is generally known as the chief audit executive (CAE). A senior manager and soon-to-be CAE who has been challenged to establish a new internal audit function is faced with a variety of options, depending on the enterprise's overall business, its geographic and logistical structures, the control risks it faces, and the overall enterprise culture. Whether a corporation structure with a requirement for an audit committee or some other type of enterprise, there is almost always a need and reason to establish an internal audit function. This section discusses some of the elements required to build and manage an effective internal audit organization.

A key requirement for any effective organization is a strong leader; for internal audit, that leader is a CAE who understands the needs of the overall organization and its potential control risks as well as the potential contributions that internal audit can make. This person must have the support of both the audit committee and senior management. Most large enterprises today have multiple units often spread across the world and with many different business activities. Even if geographically positioned in one location, the larger enterprise almost always has multiple specialty functions with control risks that may require separate internal audit emphasis. The effective internal audit department must be organized in a manner that serves senior management and the audit committee by providing the best, most cost-effective audit services to the entire organization. We consider the benefits and difficulties in having a centralized or a decentralized internal audit organization as well as some alternative internal audit organizational structures.

As before, this chapter refers a hypothetical example company, Global Computer Products. This relatively small IT software and hardware manufacturer and distributor, mentioned in other chapters as well, is headquartered in the United States but with some worldwide operations. We assume here that the company was incorporated not too long ago, did not come under SOx registration requirements because of its size, and never had an effective internal audit function. Management and a newly formed audit committee have decided that Global needs to launch an effective internal audit function.

12.2 Audit Charter: Audit Committee and Management Authority

An internal audit charter is a formal document, approved by the audit committee, to describe the mission, independence, objectivity, scope, responsibilities, authority, accountability, and standards of the internal audit function for an enterprise. Internal audit has free rein to look at a wide range of records and to ask questions at all levels. Internal auditors have a lot of authority in an enterprise, and some type of

authorizing authority is needed. Because the internal function should report to the audit committee of the board in a corporate structure, that audit committee normally should authorize the rights and responsibilities through a formal authorizing document or resolution—usually called an internal audit charter.

There are no fixed requirements for such an authorizing document, but an internal audit charter should affirm internal audit's:

- Independence and objectivity
- Scope of responsibility
- Authority and accountability

This charter, then, is the authorizing document that an internal auditor can use when a manager in a separate and sometimes remote organizational unit questions why an internal auditor is asking to review certain documents or to gain access to some enterprise facility. The charter says that senior management—the board of director's audit committee—has access to enterprise records. More important, the charter provides a high level of authorization for the enterprise's internal audit function.

There is no fixed format for the contents of a charter. The internal audit standards of the Institute of Internal Auditors (IIA), as discussed in Chapter 8, refer to the need for an internal audit charter, but the IIA's Web site (www.theiia.org) does not provide that much specific guidance. A general Web search for internal audit charters provides a variety of posted examples, but these are primarily from government and academic institutions. Exhibit 12.1 is an example internal audit charter for our Global Computer Products example company. It clearly outlines internal audit's authority as well as such responsibilities as developing a risk-based audit plan and issuing timely audit reports. All of these are discussed in other chapters as part of an internal audit CBOK.

An internal audit charter is little more than an impressive looking document unless there is a strong internal audit function in place to launch and perform these key internal audit activities: understanding the areas in any enterprise that should be candidates for internal audit reviews, building an effective internal audit organization and team, and establishing supporting procedures to allow those internal audits. While an internal audit charter is an essential authorization to launch a new internal audit function, many if not most internal audit functions today have a charter that may have been developed and approved in the past but has not been recently reviewed and updated. If one is in place, the CAE should periodically review the existing charter and present it to the audit committee to reaffirm the members' understanding of the role and responsibilities of internal audit.

12.3 Building the Internal Audit Staff

With the exception of a very small single-person internal audit function, every internal audit function needs to have someone in charge and responsible for internal audit—the CAE as well as some supporting and administrative staff. While there can be many variations in position descriptions and titles, this section provides some model internal auditor position descriptions for various levels and types of internal auditors in an enterprise. Those same position titles will map to the various internal audit organization structures discussed later in the chapter. In addition, there are different CBOK requirements for each of these internal audit position descriptions.

EXHIBIT 12.1 Sample Internal Audit Charter

Global Computer Products

Internal Audit Department

Authorizing Charter

Internal Audit's Mission

The mission of Global Computer Products Internal Audit is to ensure that company operations follow high standards both by providing an independent, objective assurance function and by advising on best practice. By using a systematic and disciplined approach, Internal Audit helps Global Computer Products accomplish its objectives by evaluating and improving the effectiveness of risk management, internal control, and governance processes.

Independence and Objectivity

To ensure independence, Internal Audit reports directly to the Board of Directors Audit Committee, and to maintain objectivity, Internal Audit is not involved in day-to-day company operations or internal control procedures.

Scope and Responsibilities

The scope of Internal Audit's work includes the review of risk management procedures, internal control, information systems, and governance processes. This work also involves periodic testing of transactions, best practice reviews, special investigations, appraisals of legal and regulatory requirements, and measures to help prevent and detect fraud. To fulfill its responsibilities, Internal Audit shall:

- Identify and assess potential risks to the Bank's operations.
- Review the adequacy of controls established to ensure compliance with policies, plans, procedures, and business objectives.
- Assess the reliability and security of financial and management information and supporting systems and operations that produce this information.
- Assess the means of safeguarding assets.
- Review established processes and propose improvements.
- Appraise the use of resources with regard to economy, efficiency, and effectiveness.
- Follow up recommendations to make sure that effective remedial action is taken.
- Carry out ad hoc appraisals, investigations, or reviews requested by the Audit Committee and Management.

Internal Audit's Authority

In order to promote effective controls at reasonable cost, Internal Audit is authorized, in the course of its activities, to:

- Enter all areas of Global Computer Products operations and have access to any documents and records considered necessary for the performance of its functions.
- Require all members of staff and management to supply requested information and explanations within a reasonable period of time.

Accountability

Internal Audit shall prepare, in liaison with management and the Audit Committee, an annual audit plan that is based on business risks, the results of other internal audits, and input from management. The plan shall be presented to senior management, including the General Counsel, for approval by the Audit Committee. Any needed adjustments to the plan should be communicated to and approved by the Audit Committee.

Internal Audit is responsible for planning, conducting, reporting, and following up on audit projects included in the audit plan and for deciding on the scope and timing of these audits. The results of each internal audit will be reported through a detailed audit report that summarizes the objectives and scope of the audit as well as observations and recommendations. In all cases, follow-up work will be undertaken to ensure adequate response to internal audit recommendations. Internal Audit also will submit an annual report to senior management and to the Audit Committee on the results of the audit work including significant risk exposures and control issues.

Standards

Internal Audit adheres to the standards and professional practices published by the Institute of Internal Auditors as well as the Information Technology Governance Institute.

(a) Role of the CAE

Someone should be responsible for any internal audit function—this is usually the boss. Although the title internal audit director was common in years past, IIA standards today support the title of CAE, the most senior audit officer in the enterprise with ultimate responsibility for the entire internal audit function. SOx also has increased the importance of the CAE as well as the internal audit function. As was discussed in Chapter 4, the internal audit function of a SOx-registered enterprises must report to the audit committee, and a CAE would be the single person in the enterprise to represent internal audit plans and work with the audit committee.

No matter whether the business is a large Fortune 50 major corporation or a relatively small private or not-for-profit enterprise, the CAE is the person to lead and direct internal audit. While we are presenting a sample CAE position description here, the CAE should be responsible for the following areas. These topics should be part of any CAE's CBOK and also be reflected in the internal audit charter.

- **Enterprise operations and risk issues.** In addition to managing the internal audit function, the CAE should have knowledge regarding all aspects of the enterprises operations, whether financial, logistical or operational matters.
- **Human resources and internal audit administration.** The CAE is responsible for the internal audit staff and must build an effective organization and both recruit and lead an effective internal audit team.
- **Relationships with the audit committee and management.** The CAE is the internal audit spokesperson for the audit committee and all levels of enterprise management.
- **Corporate governance, accounting, and regulatory issues.** Whether it is SOx, accounting, finance issues, or other regulatory matters impacting the enterprise, the CAE should have at least a general understanding and knowledge.
- **Internal audit team building and administration.** No matter what size the team is, the CAE is responsible for building an effective internal audit function that is respected by recipients of internal audit services.
- **Technology.** The CAE should have a general understanding of how technology is used within the enterprise as well as how it can be applied to promote internal audit services.
- **Risk-based audit planning and process excellence.** The CAE should understand risk assessment processes, as they are applied to enterprise operations, and also should be able to think of operations in terms of key processes.
- **Negotiating skills and relationship management.** The CAE often will be involved with issues raised by the internal audit team and a sometimes hostile management, which may take exception to internal audit's findings and recommendations. The CAE often must negotiate an appropriate resolution to these issues as part of building an effective internal audit team.
- **Internal audit's assurance and consulting roles.** Although these roles sometimes can become blurred, the CAE should always emphasize to both the internal audit team and management the distinctions between the separate roles of providing internal audit assurance services and providing consulting services.
- **Standards for the professional practice of internal auditing.** The CAE should be an expert on these IIA standards and should help to apply them to all aspects of internal audit activities.

The CAE has an important job in both leading an effective internal audit department and delivering internal audit services to the enterprise. Although many members of the internal audit team may have stronger or more specialized knowledge is some areas, the CAE is the key person who represents internal audit to the enterprise.

(b) Internal Audit Management Responsibilities

Depending on the overall enterprise size, an internal audit function may have multiple levels of supervisors or managers to manage the internal audit function. These resources create an effective internal audit function through close planning, monitoring, and supervising the field audit staffs that are actually performing internal audits. While the CAE should be an internal audit generalist with a good knowledge of enterprise internal controls issues and internal audit practices, the internal audit managers and supervisors generally are specialists in such areas as financial or IT internal audit issues. As an example, Exhibit 12.2 is a sample position description for an internal audit manager with financial audit skills. Such an internal audit manager often would be expected to have a certified public accountant (CPA) designation in addition to a certified internal auditor (CIA) designation to enable him or her to better communicate and understand finance and accounting issues with both enterprise management and the internal audit staff.

We perhaps too often insist that a certification such as a CPA, CIA, or certified information systems auditor (CISA) is a *requirement* for certain types of internal audit positions. While certifications certainly are measures of demonstrated skills, a CAE building an effective internal audit organization should always consider the skills and aptitudes of the candidates for any internal audit manager position rather than just the initials after their names. For example, an internal audit staff member may have joined an enterprise internal audit group with a bachelor's degree in economics. If he or she joined the internal audit department, acquired a CIA, and performed well in accounting and financial internal control audits, a lack of a CPA should not necessarily prevent that person from being a candidate for an internal audit manager performing financial reviews.

Enterprise human resource functions may impose requirements here, but the CAE should insist that appropriate positions descriptions are in place for all members of the internal audit management team. The teams should be structured in such a manner that all members of the internal audit staff can recognize the requirements to move from one level on up to the next. For example, an internal audit field supervisor should clearly understand the additional requirements to move up to an internal auditor manager level if such a position becomes available and open.

(c) Internal Audit Staff Responsibilities

In many enterprises, internal audit is an excellent entry place for new nonspecialist staff members who are just out of college. That is, an enterprise may have requirements for engineers and will want to hire new engineering degree graduates or may have needs for people in advertising and will want to add new candidates with appropriate advertising or communications skills, but entry-level staff internal audit candidates can come from a wide range of college degree areas. Many general

EXHIBIT 12.2 Internal Audit Manager Position Description

Job Responsibilities
The Manager, Financial Internal Audit has responsibility for assisting the Chief Audit Executive (the "Director"), in providing guidance and supervision of the Internal Audit Department (the "Department"). Additionally, the Manager, Financial Internal Audit is responsible for: (1) executing the financial/operational audit portion of the Department's Annual Audit Plan, (2) assisting the Director in preparing regular updates of financial internal audit activity to the Audit Committee, (3) providing advice and counsel on new systems, initiatives, and services under development from an internal controls perspective, (4) assisting the Director in the coordination of financial internal audit activities, including Sarbanes-Oxley Section 404 internal controls assessments, with the independent registered public accountants, (5) effectively and efficiently managing financial internal audit function resources, (6) hiring, training, and professionally developing the financial internal audit team, and (7) overseeing the quality of work performed by the financial internal audit team, ensuring compliance with applicable standards.

Financial Internal Audit Manager Key Competencies
- In-depth knowledge of internal audit practices and principles including IIA standards
- Strong knowledge of accounting principles and a thorough understanding of financial statements
- Solid knowledge and experience with regulatory rules and requirements affecting the internal auditing and accounting professions (e.g., Sarbanes-Oxley Act)
- Detail oriented with strong analytical and problem solving abilities
- Solid leadership, management, and administrative skills
- Broad-based business knowledge including financial/operational practices and procedures from a company operations perspective
- Strong interpersonal, communication, and presentation skills

Required Skills
- **Bachelor of Science degree** in Business Administration with a major in Accounting or Finance
- A minimum of **seven years** of progressive internal audit and/or public accounting experience
- Both a **Certifie Public Accounting (CPA) and** a Certified Internal Auditor (CIA) **designation.**

degree programs, such as those in finance, accounting, economics, or information systems, can provide good internal auditor candidates. An excellent source for such candidates are colleges that offer specialized bachelor-level internal audit degree programs. The program at Louisiana State University[1] is an excellent example of a well-regarded internal audit training program. Students there receive a bachelor's degree in internal auditing.

Candidates for an entry-level internal audit position do not necessarily need to just have an accounting degree, the historic typical entry point for many internal auditors, but should have a strong ability to understand IT systems and process flows coupled with superb speaking and writing skills. Even at a staff level, a beginning internal auditor should be someone who can quickly review often complex processes, assess any potential weaknesses, and then communicate those concerns to internal audit management and overall enterprise management.

Exhibit 12.3 is a position description for an entry-level operational internal auditor. This type of candidate does not necessarily have strong CPA-like accounting

EXHIBIT 12.3 Staff Internal Audit Position Description

Job Responsibilities

As a member of the Corporate internal audit department and under the direction of an assigned internal audit manager, a staff internal auditor is responsible for planning, developing, performing, reporting, and following up on specific internal audit assignments as directed. Staff internal auditor responsibilities must be carried out in accordance with internal audit department procedures, following IIA *Standards for the Professional Practice of Internal Auditing*.

Specifi Duties and Responsibilities

- Prepare or revise audit programs to accomplish objectives, and perform internal audits in accordance with approved audit programs.
- Review and appraise the soundness of internal controls and determine the adequacy of these controls.
- Conduct periodic reviews and tests to ensure compliance with procedures and regulatory requirements, making recommendations for improving current and proposed procedures.
- Review and report on possible internal controls weaknesses and violations of corporate business practices, policies, or procedures.
- Perform other job-related internal audit duties as assigned.
- Attend internal/external meetings to expand professional expertise and maintain professional contacts that support assigned functions.

Knowledge and Skills

- **Education:** B.S. degree or the equivalent of experience and education.
- **Interpersonal Skills:** A significant level of trust and diplomacy is required, in addition to normal courtesy and tact. Work involves extensive personal contact with others and/or is usually of a personal or sensitive nature. Work may involve motivating or influencing others. Outside contacts become important and fostering sound relationships with other entities (companies and/or individuals) becomes necessary.

Other Skills

- General knowledge of accounting and audit procedures and the ability to work independently
- A working knowledge of spreadsheets and word processing software; able to operate a laptop computer and general office equipment
- Able to work independently

and auditing skills but rather is someone who can understand and analyze business processes, perform tests, develop descriptive documentation, and make appropriate recommendations. This staff-level operational audit position can be an entry-level slot into the internal audit function. Of course, if a new candidate has a degree in internal auditing, has passed at least portions of the CPA or CIA examinations, or did some internal audit work in another enterprise, he or she should be brought in on a slightly more senior level.

Where does such an entry-level position lead? Internal auditors often must have specialized knowledge in accounting and finance or other specialized areas. Much of this knowledge can be gained through a strong program of training seminars or on-the-job experience. As discussed later in this chapter, an internal audit function

should implement a strong and ongoing training program for all members of the internal audit function.

(d) Information Systems Audit Specialists

Although many staff internal auditors can be successful in an enterprise with only general knowledge and can learn much more through training, IT specialist internal auditors need special training and skills. Most if not all internal audit functions need at least one specialist on the internal audit staff with strong IT-related internal control skills covering such areas as systems security, application internal controls, and computer systems operations management. Many additional internal audit knowledge needs are discussed in Part Five. This type of internal auditor skill requirement goes beyond entry-level positions where an auditor candidate has a bachelor's degree in computer science and an understanding of spreadsheets but not much more IT-related knowledge.

The skill requirements for the information systems audit specialists in an internal audit group will very much depend on the technical maturity of the enterprise's IT functions. An enterprise with applications based on an enterprise resource planning set of linked applications tied to complex databases will require a different set of information systems audit specialist skills than would an enterprise where most IT resources are Web-based applications. Due to the span and breadth of ever-changing IT technologies, information systems auditors face a wide range of knowledge requirements. Exhibit 12.4 outlines the basic knowledge requirements of seasoned information systems audit specialists. These knowledge requirements are outlined in greater detailed in Part Five.

Finding and recruiting an internal auditor with information systems skills and knowledge sometimes is a challenge. It is often difficult to find professionals with the appropriate technical skills and then to identify the better candidates. Internal audit hiring managers or CAEs who have come from a CPA-oriented finance and accounting background sometimes have difficulty in identifying appropriate candidates. Of course, if the internal audit function has already established an information systems audit function, peer-level interviews for the recruitment process are great helps. An enterprise may seek candidates who have achieved certified information systems auditor (CISA) credentials. These and other internal auditor professional credentials are discussed in Chapter 27.

In addition to the IT information systems internal auditor controls requirements outlined in Exhibit 12.4, every member of an internal audit function—from the CAE to junior staff auditors—should have some CBOK level of knowledge covering IT internal control procedures. With the almost pervasive use of automated and Web tools today, such knowledge is fairly common, but some otherwise competent internal auditors sometimes tend to avoid IT technical matters. In the concluding chapter of this book, Section 34.1 outlines a set of CBOK information systems knowledge requirements for all internal auditors.

(e) Other Internal Auditor Specialists

Typical internal audit positions range from the CAE in charge of the function, supporting internal audit managers, internal audit staff, and information systems audit specialists. However, depending on the size of the enterprise and the overall nature

EXHIBIT 12.4 Information Systems Auditor Basic Knowledge Requirements

Note: Information technologies are pervasive in business and span a wide range of options and technologies. However, an information systems internal auditor should be expected to have at least a high-level working knowledge of these areas:

- Business application systems—whether for accounting, business, or other purposes—and the basic balancing and integrity controls surrounding all automated systems
- Data management processes—whether a formal database or spreadsheet tabled data—and the importance of validating and maintaining that data
- Systems development life cycle (SLDC) processes to implement and build business application systems
- Storage management and the importance of backup and recovery processes.
- Computer operating systems basic functions—whether on a laptop system or larger system—and the potential risks and vulnerabilities if such systems are not updated or maintained
- Computer systems architectures, with an emphasis on use of the Web, client-server configurations, and telecommunications
- IT service operations processes, with an emphasis on problem management, access controls, and general application management
- IT service design processes, with an emphasis on continuity, capacity, and information security management processes
- Governance and service strategy processes, including essential IT financial management processes.
- Programming or coding techniques sufficient to construct and implement computer-assisted audit procedures appropriate to the enterprise environment
- Ongoing interest and curiosity to understand and explore newer and evolving technology concepts, such as storage management virtualization

of internal audit activities, there can be other specialty positions in internal auditor support roles. Much depends on how the responsibilities of internal audit have been defined through its charter. For example, IIA standards define the roles where internal auditors can act as in-house consultants to their enterprises and when they can act as assurance-level internal auditors. Some enterprises may want to expand that role and establish a full in-house consulting practice as part of internal audit's activities. Chapter 28 discusses this role of an internal auditor as an enterprise consultant.

Similarly, there is another other branch of internal auditing called quality auditing. These internal auditors are more oriented to the production shop floor and follow a complementary set of standards from the American Society for Quality in the United States. Quality auditors traditionally have operated as a totally separate function from IIA-oriented internal auditors. However, we are beginning to see a greater integration between these two audit functions. Quality assurance auditing is discussed in Chapter 31.

In addition to internal audit specialists, an enterprise may want to add other support personnel to the internal audit group for such tasks as monitoring and organizing internal controls documentation; larger internal audit groups may need staff just to support the laptop computers and other resources need by the group as a whole. These other professionals support internal audit's overall mission to review

and help improve internal controls in the enterprise: the real purpose of an effective internal audit function in an enterprise.

12.4 Internal Audit Department Organization Approaches

There is really no optimal way to organize an internal audit function. Much depends on size, nature of internal controls, and span of the enterprise activities as well as the overall objectives of internal audit, as outlined in an approved internal audit charter. Logistics and costs are often other key factors. An enterprise with significant worldwide operations may need internal auditors available to perform reviews on-site at those worldwide operations. Internal audit can be organized in a decentralized manner with a local team available to be close to actual operations. The risks here are that it may be difficult to a CAE to organize a unified enterprise-wide internal audit function, and local internal audit functions can become almost divorced from the headquarters CAE-led internal audit function. However, those local internal auditors can observe local operations and be on-site quickly, without the delays of travel time.

If the internal audit function is primarily based at headquarters, a team of home office internal auditors would have the responsibility to visit the site to perform their audits. This approach encourages more consistent internal audit operations but may result in travel and scheduling costs. In addition, sometimes maintaining a team of internal auditors who are willing to travel at great deal is challenging. There is no simple answer here, and the next sections discuss strategies for building an effective internal audit function.

(a) Centralized versus Decentralized Internal Audit Organization Structures

Up until perhaps the mid-twentieth century, many enterprises were managed and organized in a highly centralized manner. Major decisions were made by a central authority, and lower-level enterprise personnel did little more than pass materials up through the ranks for central office approvals. Perhaps the best modern example of such a highly centralized organization structure would be the Soviet Union before its collapse in the late 1980s. There, most planning and economic decisions theoretically were made by a limited number of central authorities. A production plant with a need for pencils, for example, for the upcoming year would have to list its requirements for pencils into an annual production plan. Assuming that the plan was approved by the central authorities, the plant would then file supply requisitions covering its needs for pencils over the course of the planning cycle, often for as long as five years. The central planning authority would look at all of the requests for pencils from plants and offices across the country to decide both how many pencils were to be manufactured in order to supply everyone and how many trees should be cut down to supply raw materials for those wood pencils.

While this type of central planning sounded very efficient to the idealist, most societies today know such highly centralized planning just does not work. Large economic units find it difficult, if not impossible, to develop appropriate centralized plans to correctly define the requirements or set the rules for everyone. Too many persons spend time processing approval documents, and the ultimate users of the services do not see much value from the process. We also saw a similar

example of the failure of central planning when the U.S. federal government tried to regulate prices and allocate the supply of gasoline in the late 1970s. The result was high prices, long lines due to local shortages, and an army of bureaucrats trying to write and rewrite rules. Prices went down and oil supplies increased only after central controls were abolished in the early 1980s. Today, many enterprises that once were highly centralized have pushed decision-making authority down and have decentralized many of their processes. Modern larger enterprises are extremely decentralized, with each operating unit responsible for making most of its business decisions, including securing its own financing.

Whether the internal audit function is organized for the total enterprise or not, a major decision is whether individual internal audit decisions should be made at lower or local levels, as opposed to those requiring approval by a central authority. For internal audit, the kinds of decisions and actions involved may include modifiying required audit procedures, procedures necessary to report deficiency types, negotiations necessary to take actions on audit findings, the manner of reporting audit findings, and internal auditors' follow-up on corrective action taken to fix reported deficiencies. The arguments or benefits that support decentralization generally include:

- Freeing up personnel from minor decisions so that they can deal with more important matters. Senior management does not always need to review or approve these less significant details and can become mired in lower-level details, missing important overall management audit strategy decisions.
- Local unit personnel often have a better understanding of local problems. Rather than summarizing problem situations and passing them up to higher levels for decision making, local unit management often can act directly and in a more rapid and intelligent manner.
- Delays involved in passing decisions up for approval can be avoided. Local unit personnel are often better motivated to solve problems at their own level of the organization and often will have the opportunity to develop more appropriate decisions.

Local unit internal audit groups that make decisions at a local level are often viewed with more respect by other local unit personnel. Despite these observations favoring decentralized structures, however, there are also strong arguments in favor of a centralized or headquarters internal audit function that performs internal audits throughout the enterprise, including:

- The Committee of Sponsoring Organizations (COSO) internal controls framework and SOx rules (see Chapters 3 and 4) very much promote the importance of tone-at-the-top messages from senior management at multiple levels. A centralized internal audit enterprise can be in a strong position to deliver such senior management messages to the field units it is reviewing.
- Separate audit groups may not know the full implications of some corporate policies and decisions. This is particularly true where communication links to remote internal audit groups are weak. Decentralized-enterprise field auditors may have problems explaining the rationale behind certain central policy decisions or have trouble adequately communicating those decisions. A centralized audit group may do a better job here.

- A centralized internal audit enterprise generally finds it easier to maintain uniform, enterprise-wide standards. These standards can be established through strong internal audit common policies and procedures and through messages communicated via e-mail, conference calls, and other tools.
- A decentralized internal audit function may sometimes forge too-strong loyalties to their local reporting units. The local audit manager can become more loyal to a plant or division manager where the local audit function is located rather than to the CAE.

While this discussion assumes that an internal audit function is either highly centralized or highly decentralized, there are numerous in-between positions and other variations where some matters are delegated and others are not. Many internal audit functions can keep certain specialized functions at headquarters, reporting to the CAE, with other more operational audit units at division or unit headquarters. It is not practical to suggest a single best solution to these alternatives, and the CAE should have the responsibility for organizing internal audit in a manner that best suits the needs of the enterprise.

Complex enterprise organizations often have an influence on the way internal audit is organized. A special kind of decentralization of authority exists, for example, when separate internal audit groups are units of the overall enterprise that are not part of the regular or central internal audit function. These separate internal audit functions, which may be the result of a restructuring or an acquisition, often report directly to the management of individual subsidiaries and divisions. Often here the central internal audit function serves only in an advisory capacity; many of the administrative considerations discussed in this chapter are not directly involved. This situation can occur when enterprise A owns perhaps 55% of enterprise B, with the other 45% held by other parties. Enterprise B also may have its own audit committee and CAE. However, A's 55% ownership of B means that A's CAE has some responsibility for the audit function at B as well.

The CAE for the parent enterprise (A in the example) should have a special professional concern regarding the effectiveness of the semiautonomous internal audit groups that goes beyond the normal interest in the effectiveness of all enterprise operations. This special relationship normally can be seen on complete internal audit enterprise charts, which show these other groups as reporting to the central CAE on a dotted-line basis. In these situations, the existence of the semiautonomous internal audit group's responsibility to local management does not preclude the headquarters or parent internal audit department from making supplementary reviews of these subsidiaries and divisions, as necessary.

A central internal audit function cannot be responsible for enterprise-wide internal audit results unless it has both access and line control over all supplementary internal audit work. The central CAE has a responsibility to make any dotted-line reporting relationships to other internal audit groups as strong or as weak as necessary, given overall enterprise considerations.

(b) Organizing the Internal Audit Function

Organizing an effective and efficient internal audit function presents a number challenges. Often an internal audit function was launched in the pre-SOx "old days" when internal audit was primarily a compliance review function reporting to the

controller. It is a good idea today for the CAE, with audit committee approval, to review the current internal audit charter and its organization, and to make any necessary changes. Although there may be many minor variations, internal audit functions commonly are organized in one of four ways: types of audits performed; internal audit conformance to the general structure of the enterprise; audit organization by geographical area; and combinations of these approaches with a headquarters staff. Nonaudit and informal staff assignments are also possible.

(i) **INTERNAL AUDIT ORGANIZATION BY TYPE OF AUDIT** Internal audit can be organized by the types of audits to be performed. An audit department might be divided into three groups of specialists: information systems or IT auditors, financial audit specialists, and purely operational auditors. This approach rests on the logic that individual internal auditors may be most effective if given responsibility for an area in which they have expertise and experience, recognizing that efficiency often is achieved through specialization. The problems and control risks pertaining to a particular audit area often are best handled by assigning internal auditors who have the necessary special expertise. For example, an enterprise may have a number of district and regional sales offices that all have the same kind of operations. That internal audit function may want to develop a special internal auditing group that does nothing but audit these sales offices. The practical benefits here can be substantial.

At the same time, internal audit management should recognize that there are disadvantages to this type-of-audit approach. Where several types of audits exist at a given field location, it may be necessary for each specialist internal auditor to travel to that location. This extra cost in time and money should be clearly offset by the added efficiency gained from the several specialist internal auditors. Exhibit 12.5 is an organizational chart illustrating an audit specialty internal audit organization. It shows specialized audit groups for operational, financial, and IT as well as a team for special internal audit projects. A risk with a specialized type of audit approach is that specialist internal auditors may spend too much time on their own areas and miss the big picture in overall audit process requirements. This is particularly true with technical, IT-audit areas, where auditors may spend too much time on technical

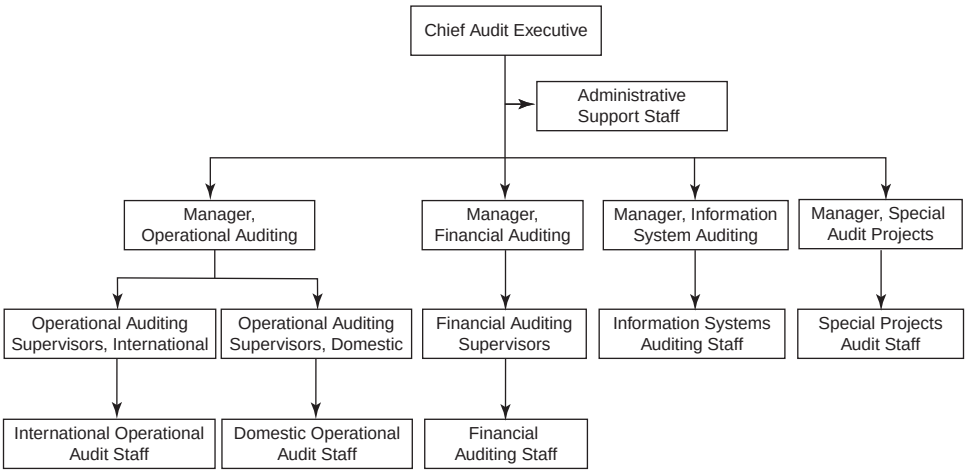


EXHIBIT 12.5 Specialty-Based Internal Audit Organization

control issues and miss significant control-concern risks. It is often very difficult for the CAE to create a team of integrated auditors with this type of approach.

Although a tight, specific definition of audit tasks can promote efficiency and allow for more effective, specialized audits, a variety of assignments keeps an internal auditor from getting in a rut and performing audit reviews in too mechanical a fashion. Here the audit staff is alert and well motivated and can bring a fresh approach to old problems—something that frequently pays good dividends. Mixed assignments for individual internal auditors lend themselves best to growth and professional development. They help to create a concept of the *integrated auditor*. This integrated audit approach promotes adequate education and training opportunities to all members of the audit staff.

On balance, any gains through audit specialization may be more than offset by the factors just discussed. Internal audit management faces the danger that these gains will appear to be more substantial than they actually are. The specialist approach should be used cautiously and only when the enterprise has strong needs for auditors with unique abilities. In many instances, this type of internal audit organizational structure is at odds with the objective of achieving maximum quality of the audit effort, especially as the concern of internal audit moves further away from reviewing lower-level procedures and toward broader managerial issues.

(ii) INTERNAL AUDIT PARALLEL TO OVERALL ENTERPRISE STRUCTURE In a large enterprise, a practical alternative is to align the internal audit organization along the same lines as the enterprise organization structure. Individual internal audit groups can be assigned to specific organizational components, such as operating divisions or affiliated subsidiaries. When these operating units are in specialized lines of business or geographical areas, internal audit may benefit from having a strong understanding of audit and control issues for those particular types of operational activities; this also leads to the development of greater internal audit enterprise-specific expertise. An example might be a large manufacturing enterprise that has a separate finance subsidiary responsible for financing equipment leases. Because of significant differences in control issues between manufacturing operations and those of the finance operations, internal audit management might find it effective to have two separate audit groups, one to cover manufacturing operations and the other for the financial subsidiary.

An advantage to this approach is that management in charge of the various operations and other operating personnel can develop more effective working relationships with internal audit personnel. The separate internal audit groups should come to speak the language of the particular operation and can become more useful to the individual management groups. Internal audit can also develop more effective working relationships with responsible managers at all levels. There are, however, certain disadvantages to this form of internal audit enterprise structure, similar to those of the type-of-audit approach just discussed. Just as separate information systems and manufacturing auditors might travel to and perform audits of the same general area, here a manufacturing division and a finance division auditor might each be asked to review the same general area if multiple operating divisions are located there. Although enterprise operating units may often be separate and autonomous, this approach can result in duplication of field travel, diminished internal audit staff motivation, and reduced opportunities for management development. A given operating division can be considered to be less important to the overall

enterprise, and members of the internal audit team assigned there may feel that their career opportunities are hampered. Another potential danger with this approach is that the separate internal audit groups can develop too close an alliance with the divisional or staff personnel they audit, which has the risk of undermining the independence and objectivity of the individual internal auditors.

The effectiveness of this internal audit organizational structure approach is more controversial than it first appears, and the method should be used cautiously. Even a very large enterprise, with many different operating units, may find it more effective to have a central group of *corporate auditors* who perform their reviews at all units, rather than by line of business. The enterprise with multiple internal audit groups, each serving separate lines of business, may find it difficult to conduct audits throughout the enterprise that speak in the same voice, no matter how strong the central internal audit policies and procedures.

(iii) GEOGRAPHICAL APPROACHES TO THE INTERNAL AUDIT ORGANIZATION Under the geographical approach, all enterprise operations in a given locale are assigned to a designated group of internal auditors. In some cases, this geographical approach automatically becomes, to some extent, a type-of-audit or enterprise-structure approach when particular types of operations are concentrated in separate geographic areas; usually, however, there is some diversity of audit assignments in the individual areas.

The advantages and disadvantages of an area approach to internal audit are similar to the first two organizational structures discussed previously. On balance, a geographic approach often seems to be best and is commonly used in practice. The number of separate audit offices to be established will depend on the scope of the enterprise's operations. In some enterprises, there may be a number of separate audit offices within the home country, with international operations located in one separate office, often at a prominent offshore location. Enterprises with a large, diverse number of international operations may have multiple international internal audit offices.

(iv) USE OF A HEADQUARTERS INTERNAL AUDIT STAFF The three approaches to organizing internal audit activities just discussed should always be supported by some kind of headquarters function. At its minimum, this may consist of the CAE and a very limited administrative support staff, with any expansion of the central internal audit function above this minimum depending on what work is delegated to the line components and the types of internal audit services provided by the central unit. In a typical situation, all or almost all audit reports may be reviewed and approved at the central headquarters. Other matters requiring centralized attention, such as common internal audit policies and procedures, may be developed, or at least finalized and distributed, by the headquarters internal audit function. There may also be some planning and administrative work that either must be or preferably is done at the enterprise headquarters. Most of these activities will require some administrative support. Other activities may be performed in part by the CAE but will usually require additional professional internal audit assistance, which might be provided by one or more headquarters internal audit managers or other planning and administrative personnel. Normally the CAE will want one individual to have the authority to act in his or her absence, thus ensuring a needed continuity of operations.

With a highly decentralized enterprise where most of the internal audit activity takes place by division, by type of audit, or by geographic area, this central internal audit function may be viewed as little more than a central corporate overhead type of function that contributes to expenses of the operating units but provides little value. Although the CAE reports to the audit committee and speaks to senior management, both may question how familiar that audit executive is with field or operating-unit audit activities. A centralized internal audit function may not be particularly effective if it does not add value to total internal audit efforts.

(v) NONAUDIT AND INFORMAL STAFF ASSIGNMENTS Internal auditors often are asked by senior management to carry out special financial or operational audit or consulting activities, even though those activities are sometimes so much a part of the regular day-to-day enterprise activities that they do not meet the test of true internal auditing. These are often task force projects of limited duration, such as solving an overall inventory control problem. The internal auditors assigned may be pulled from their regular audit assignments to participate on the project and then return to internal audit when complete.

Although such activities may delay completion of the audit plan and cause various enterprise control problems, these short-term special projects are generally good for both internal audit as a whole and for the individual auditors assigned. Senior management's desire to have internal audit participate on a special project represents an endorsement of the professionalism of all members of the internal audit enterprise. The CAE should actively encourage these types of projects periodically to give staff additional experiences and perhaps to groom them for other positions within the enterprise.

A different problem arises when management asks internal audit to assume some nonaudit function on a regular, recurring basis. Illustrative would be the responsibility for reviewing and approving current cash disbursements before those disbursements are actually made. Management may assume that because internal audit has certain special control skills, it is the best suited function in the enterprise to perform these special tasks. These types of ongoing special projects generally take resources away from regular internal audit activities and may even compromise the independence of internal audit. The CAE should strenuously object to such ongoing assignments. Assuming that internal audit has no alternative other than to accept such an assignment, the recommended organizational approach should be to segregate these additional activities from the normal internal audit activities and to subject them to periodic reviews by the regular internal audit group. Wherever possible, this kind of situation should be avoided. The dual responsibilities tend to infringe on the time for internal audit management activities. In addition, there is the very real danger that the dual responsibilities will weaken the image of the CAE to others in the enterprise.

This discussion of internal audit organizational arrangements has dealt chiefly with formal types of structures and the essential guidelines for efficient operations. In some enterprises, various kinds of interrelationships in the internal audit department may cut across the established organizational lines. Such interrelationships are informal and take place as necessary to meet current operational needs. They exist under all types of formal arrangements. Within reasonable limits, these informal organizational arrangements serve a useful operational purpose and often point the way to needed formal enterprise modifications. If carried too far, however, they can

undermine the effectiveness of internal audit's basic mission. The important thing, therefore, is to recognize their necessity but to keep them within sensible bounds.

It is always important to emphasize the changing nature of internal audit organizational needs along with the changing structure of the entire enterprise. As enterprise operations change, both in terms of their size and function, the organization approach followed by internal audit often also needs to be reappraised. In the last analysis, organizational arrangements are a means to an end, never an end themselves. Although this reappraisal can and should be made on a rather continuous basis, the preparation of the annual internal audit budget provides an especially good opportunity to carry out a more complete enterprise reevaluation.

Our overall point here is that there is no one optimal organizational structure for any internal audit function and that the CAE, with the advice of the audit committee, should develop a plan of organization that fits internal audit's overall objectives, as defined in its charter, and provides effective and efficient internal audit services to the enterprise. A major factor in building such an internal audit function is to have an understanding of its audit universe, or the number of potential auditable entities, prime activities, or other units that can be subject to individual internal audits.

12.5 Internal Audit Policies and Procedures

A regular step in many internal audits is for the internal auditor to request to see a copy of the approved polices and procedures for some area being reviewed. These are the kinds of things that set the rules for some area of operations and provide the basis for internal audit's assessment of controls there. However, consistent with the old line that "the shoemaker's children have no shoes," internal audit functions often do not take the time and effort to implement their own policies and procedures.

Every internal audit function should develop a set of policies and procedures that govern its functions as guidance to the overall audit staff and as background to the users of audit services. For example, the approved internal audit charter should be readily available for all to see; it serves as a reminder of internal audit's responsibilities. Similarly, internal audit travel policies and continuing education policies should be published. While the size and content of any such internal audit procedures manual will vary depending on the size of the function and the overall enterprise, it should contain these elements:

- **Internal audit charter and other basic internal audit authorizing documents.** The material was discussed earlier in this chapter.
- **Enterprise ethics and code of conduct rules.** These enterprise-wide rules, which particularly impact internal auditors, are discussed in Chapter 24.
- **Internal audit department rules and procedures.** These are the marching order rules that cover everything from vacation policy to decorum while on the job.
- **Internal auditing standards.** These are the guidelines for performing all internal audits. Some key points as well as references for more materials include requirements for testing evidence (Chapter 9), documenting audit results (Chapter 10), and preparing internal audit reports (Chapter 17).

While much of background material on how to perform internal audits can be found in reference materials, such as this book, an internal audit function should

document this material in a manner easily understood by all members of the internal audit department. Our examples here are in a paper format, although we would normally expect to find this material in a soft-copy format as read-only files located in internal auditor laptop computers.

As an example of an internal audit procedure, Exhibit 12.6 is a procedure page for preparing audit program, taken from the Global Computer Products example company. Audit procedures will vary depending on the philosophy and technical expertise of the audit department. However, to achieve effective coverage, the audit procedures should be consistent with the complexity of the activities reviewed.

In addition, internal audit should establish standards for audit work papers, related communications, and retention policies. Auditors should ensure that workpapers are well organized, clearly written, and address all areas in the scope of the audit. They should contain sufficient evidence of the tasks performed and support the conclusions reached. Formal procedures should ensure that management and the audit committee receive summarized audit findings that effectively communicate the audit results. Full audit reports should be available for review by the audit committee. Policies should establish appropriate workpaper retention periods. Of course, all internal audit department standards should be based on the IIA's *Standards for the Professional Practice of Internal Auditing,* as discussed in Chapter 8.

EXHIBIT 12.6 Audit Program Preparation Procedure Sample Page

Global Computer Products

Internal Audit Standards—Preparing Audit Programs
Standard X-YYY yyyy/mm/dd

The in-charge auditor for any assigned review should gather supporting documentation and meet with appropriate managers to complete and document:

- A risk assessment process to describe and analyze the risks inherent in the selected line of business. Auditors should update the risk assessment at least annually, or more frequently if necessary, to reflect changes to internal control or work processes and to incorporate new lines of business. The level of risk should be one of the most significant factors considered when determining the frequency of audits.
- An audit plan, based on the audit committee's approved annual plan, detailing internal audit's budgeting and planning processes. The plan should describe audit goals, schedules, staffing needs, and reporting. This audit plan should be defined by combining the results of the risk assessment and the resources required to yield the timing and frequency of the planned internal audits. The internal auditors should report to the audit committee for its approval on a periodic basis the status of planned versus actual audits and any changes to the annual audit plan.
- An audit cycle that identifies the frequency of audits. Auditors usually determine the frequency by performing a risk assessment of areas to be audited. While staff and time availability may influence the audit cycle, they should not be overriding factors in reducing the frequency of audits for high-risk areas.
- Development of approved audit work programs that set out for each audit area the required scope and resources, including selection of audit procedures, extent of testing, and basis for conclusions. Well-planned, properly structured audit programs are essential to strong risk management and to the development of comprehensive internal control systems.

12.6 Professional Development: Building a Strong Internal Audit Function

This chapter has explored some of the essential beginning steps to build and maintain an effective internal audit function. Starting with an audit committee–approved authorizing charter, the designated CAE or internal audit head should build an effective internal audit organization that serves all aspects of the enterprise. Internal audit also needs to be an effective resource for the overall enterprise with its own defined operating practices, position descriptions, and appropriate policies and procedures. However, internal audit is not an outside consulting practice with any day-to-day connections; it will always be an internal function and thus must be part of that enterprise in terms of operating style and adherence to enterprise rules, such as work hours or even business attire. Nevertheless, while internal audit is part of an enterprise, we must never forget that it is always independent, unique, and special.

Internal audit is unique and special because, with the exception of the chief executive officer and sometimes the general counsel, it is usually the only unit that reports directly to the audit committee. Every employee, no matter how many levels removed down the ladder on an organization chart, theoretically reports ultimately up to that same board; internal audit is one of the few functions with direct access. Internal audit has a unique position in any enterprise as it has the right—and even obligation—to assess risks, schedule reviews in any venue of operations, and then both report the results of those reviews and request corrective actions when appropriate. This important role requires professional attention and respect from all members of internal audit.

A major theme throughout this book is the importance of an internal audit body of knowledge, a CBOK. We usually think of this internal audit CBOK in terms of the more technical aspect of internal auditing, such as SOx requirements, discussed in Chapter 4, or fraud detection and prevention, discussed in Chapter 25. This chapter, however, has highlighted a different area of internal audit CBOK needs, including knowledge of internal audit charters and an understanding of building an effective internal audit organization. An understanding of these concepts is an important CBOK skill for internal auditors at all levels.

Note

1. LSU Center for Internal Auditing, www.bus.lsu.edu/old/cia/site_from_jared_3-28/course_list.htm.

CHAPTER 13

Internal Audit Key Competencies

The overall emphasis throughout this book is on the common body of knowledge (CBOK) areas that internal auditors should know and understand. Most of these cover areas where internal auditors should gain a great knowledge and understanding, such as Chapter 8 on internal audit professional standards, Chapter 16 on documenting results through effective workpapers, and Chapter 20 on cybersecurity and privacy controls. Each of these chapters presents an overview of the subject area and points to concepts and issues where an internal auditor can gain a better understanding through additional study, experience, and internal audit activities. However, underneath this need for better understanding of the many specialized internal audit areas, all internal auditors must also establish some key professional competencies, such as the ability to conduct an effective audit interview and to operate in a professional and credible manner when conducting their internal audits. This chapter discusses these essential internal audit competencies.

Many key competency areas cover things internal auditors should have learned well before starting their careers and even while acquiring a basic education. This chapter cannot really explain how an internal auditor should conduct an auditee interview, for example, as such an interview depends on the individual internal auditor and the surrounding circumstances. However, a goal of this chapter is to remind internal auditors of subjects and areas that are professionally important to the practice of modern internal auditing.

Building an internal audit CBOK has been our ongoing chapter-by-chapter topic. The internal audit key competencies discussed in this chapter should be fundamental CBOK requirements for all internal auditors. This chapter will provide some best practices guidance on helping internal auditors establish these areas as internal audit key competencies.

13.1 Importance of Internal Audit Key Competencies

What skills are essential to be a successful internal auditor? There are many, and they include having attained at least a four-year college degree in an area that will give the new auditor an understanding of the importance of business processes as well as the ability to observe areas of operations and to describe them through written and verbal approaches. More important and even more fundamentally, an internal auditor must have strong personal ethics and a work-related commitment. That is, when sent to some location to perform a review, the internal auditor must maintain a professional demeanor and conduct his or her work in an honest and

ethical manner. These things are really fundamental and necessary to build a set of internal auditor key competencies.

We have defined internal audit key competencies as a necessary skill to conduct effective internal audits. While some professionals may look at these selections differently, adding or deleting some, our recommendation for internal audit key competencies includes:

- **Interview skills.** Whether interviewing a unit manager or staff members on a production floor, an internal auditor should be able to meet with people, ask appropriate questions, and gain the desired information.
- **Analytical skills.** An internal auditor must have the ability to look at a series of sometimes disconnected events and data and to draw some preliminary conclusions from that material.
- **Testing and analysis skills.** Related to analytical skills, an internal auditor should be able to review multiple events or populations of data to perform tests that will determine if audit objectives are effective.
- **Documentation skills.** An internal auditor should be able to take the results of audit observations and any tests of that data and document those results, both verbally and graphically, describing the environment that was observed.
- **Recommending results and corrective actions.** Based on documented testing and analysis results, an internal auditor should be able to develop effective recommendations for corrective actions.
- **Communication skills.** An internal auditor should be able to communicate the results of the audit work along with recommendations for corrective actions to the staff that was the subject of the audit and to senior management.
- **Negotiating skills.** Since there can always be a difference of opinion on internal audit findings and recommendations, an internal auditor should be able to negotiate successful final results.
- **Commitments to learning.** Internal auditors are always experiencing new changes and materials in their enterprise operations and the profession; they must have a passion for learning and continuing education.

These represent some key competencies and skills that are necessary to perform effective internal audits, no matter what industry, geographic area, or type of internal audit. The next sections discuss these key competencies in greater detail.

13.2 Internal Auditor Interview Skills

Internal auditor interviews with members of auditee management and staff are an important first step in the internal audit process. Based on an overall risk assessment and an established audit universe, as discussed in Chapter 10, an internal audit function plans to perform a review of some area, whether an assessment of internal controls, a review of operational processes, or any of many other types of internal audits. The internal audit function structures some preliminary plans for that internal audit, including identifying the audit objectives, timing, and internal audit resources to be assigned. These steps are discussed in Chapter 15. As a key part of these interview skills, the assigned in-charge internal auditor then meets with designated members of the auditee organization for an initial internal audit interview.

EXHIBIT 13.1 Internal Auditor Preliminary Auditee Interview Checklist

1. After introductions all around, internal audit should outline the timing and objectives of the planned internal audit.
2. Introduce internal auditors who will be doing actual review as well as expected auditee participants.
3. If this is the first planned audit in this area or if there have been significant changes since the last review, arrange for a walk-through of the operations area to be reviewed.
4. If there had been a past internal audit in this area, check on the status of past findings and recommendations as well as any system changes since.
5. Outline the planned timing of the audit review steps.
6. Request or make arrangements to audit materials, including:
   a. Access rights to files and IT systems resources
   b. Temporary passwords, access right to key files, and physical libraries
   c. Internal audit working space and telecommunication connections
   d. Plant parking, guard desk badges, and other facility access issues
7. For extended time period reviews, schedule periodic status meetings.
8. Schedule tentative planned audit completion as well as preliminary wrap-up meetings.
9. Make arrangements for resources available to resolve any questions or problems during the course of the review.
10. Explain the expected internal audit process, including any planned draft report, expected response times to audit recommendations, and delivery of the final report.
11. Throughout the interview and certainly here, allow sufficient time for questions.
12. Follow-up interview with a detailed summary memo outlining the potential audit timing and any matters yet to be resolved.

That initial interview and all others that follow are key steps in the internal audit process. They are valuable first steps to launch an internal audit and to gather information, but a poorly prepared or organized auditee interview can throw the internal audit so off course that it may be difficult to complete the audit as planned. All internal audit interview meetings, whether with auditee management or team associates, should be based on some internal audit planning and preparation before launching the meeting.

Once an auditee interview has been scheduled, the auditor should begin to focus on interview preparation. An internal auditor should never be fooled into thinking that she can simply walk into an auditee interview and inform them of the planned audit. The auditee manager may say that "the timing is bad," the audit objectives seem misstated, or "all of that was covered" in some past period review. An internal auditor's goal must be to demonstrate the objectives of the planned review and his or her knowledge and qualifications for the planned internal audit. Adequate preparation is key.

Exhibit 13.1 is a list outlining issues to consider when launching a new internal audit in some area that may have been reviewed in a past period. These notes have been prepared as if management on both sides is new participants in this review, and thus introductions and explanations all around are necessary.

Internal auditors will be involved with auditee and other management group meetings or interviews on a regular, ongoing basis. These meetings are the contact points to launch new internal audits as well as to review the status and continuing progress of ongoing internal audits. Such meetings are generally not formal. Often they involve an internal auditor just meeting a manager at a nearby office desk or in

a canteen over coffee. The real skill and competency need here is that an internal auditor should carefully plan objectives and even expected outcomes from such sessions and should conduct them in a planned, orderly manner. The last thing a professional internal auditor should do is to burst in on an auditee manager with no warning and just blurt out some concerns. The internal auditor's objectives will not be met in that situation, and internal audit will lose credibility in the eyes of enterprise management.

13.3 Analytical Skills

Adopting a definition from the Web source Wikipedia, *analytical skills* refers to the ability to visualize, articulate, and solve complex problems and concepts and to make decisions that make sense based on available information. Such skills include demonstration of an internal auditor's ability to apply logical thinking to gathering and analyzing information, designing and testing solutions to problems, and formulating plans. To test for analytical skills, an internal auditor might be asked to look for inconsistencies in some production report, to put a series of events in proper order, or to critically read a project status report and identify potential errors. An analytical review usually requires an internal auditor to review some audit evidence materials and then to use logic to pick apart a problem and come up with a solution.

Internal auditors are required to use such analytical processes on a regular basis in the course of their audits. The idea is not to jump into an audit with an already assumed conclusion but to break down the elements of whatever data or series of events is being analyzed in order to reach a conclusion. This conclusion may very well not always be the one the internal auditor expected to reach. To be truly analytical, internal auditors need to think about all of the factors involved in a situation and then evaluate pluses and minuses in order to develop a recommended solution.

Many audit decisions are fairly easy to make. For example, a voucher either is or is not approved or an account either does or does not balance. However, sometimes other decision criteria are not that clear cut. For example, an auditor might have the task of reviewing whether the separate documentation packages for a large set of product descriptions were adequate. While packages may be missing, causing a failed audit test for that condition, many other documentation packages may be only "sort of" in place. Here an internal auditor should develop establish some documentation adequate/not adequate decision criteria. The auditor should review all or a representative sample (see Chapter 9) on the basis of that criteria to assess documentation adequacy.

Internal audit decisions should be made in a consistent, organized manner. It is for this reason that internal auditors should view analytical skills as a key competency. Too often, some professionals think of the terms *analytics* or *analytical analysis* as a detailed, mathematical-oriented process. Internal auditors should use an analytical approach to describe their use of well-documented, well-reasoned processes to arrive at decisions in their internal audit activities.

13.4 Testing and Analysis Skills

While internal auditors should develop their initial decision approaches analytically, their next challenge and a required key competency is to have the ability to test,

EXHIBIT 13.2 Audit Testing Approaches

Physical Observation
Testing approach is used for processes that are difficult to formally document or control. For example, IT service desk problem analysis, stockroom cleanliness, or customer service practices are important to the enterprise's image but usually are not formally controlled. These factors can be especially important to organizational success when considered in broader contexts, such as assessments of employee morale or the professional tone of an office. Because these areas are somewhat subjective, developing internal audit recommendations can be difficult.

Independent Evaluations
Audit confirmations are an example of independent confirmations. While this technique *is* more common with external auditors, internal auditors sometimes find it useful as well. For example, confirmation letters can be sent to enterprise vendors to verify their compliance with some matter.

Compliance Tests
Compliance testing helps determine whether controls are functioning as intended. When conducting compliance tests, internal auditors often use one broad sample to test several items concurrently. However, multiple sample are sometimes very effective. As an example, for disbursement testing, an auditor can use one sample to test documentation and approval of disbursements, another to assess contract approvals and agreement to payments, and a third to test personal reimbursements. Such targeted tests can yield much clearer results than using one sample to test all three items.

Exception or Deficienc Testing
If a reporting system shows deficient performance, exceptions can be reviewed in detail to understand root causes and determine possible resolutions. Many process improvements require coordination with other departments or persons involved in the process; internal audit involvement in deficiency resolution frequently facilitates such coordination.

Accuracy Testing
Tests for accuracy help determine whether a reviewed processes are measuring or assessing the right things and calculating results correctly. Much of today's reporting contains significant black box elements, where the underlying calculations are embedded in computer programs and intermediate files. By using CAATT procedures and gaining an understanding of the reporting objectives, internal auditors can effectively verify systems reporting accuracy.

review, and assess the materials. Chapter 9 discusses audit sampling, with an emphasis on statistical but also on judgmental sampling. As a key internal audit competency, however, testing or sampling should be viewed in a broader perspective. For example, Exhibit 13.2 describes some alternative audit testing approaches. The first of these, physical observation, is often not thought of in terms of the concept of testing. But if an analytical approach, with established review and acceptance criteria, is used to organize an observation-based testing process, organized physical observations can be viewed as a valid testing process as well.

No matter what method is selected, internal auditors should always take appropriate steps to make certain that the samples they are testing are representative of the overall population they are analyzing. In the past, often internal auditors selected just a couple of items of audit evidence from the top or head of a group of items and then claimed their audit conclusions were based on this "sample" even though those few items selected may not have been particularly representative of the entire

population. An understanding of the sampling and testing process should be key internal audit CBOK competencies.

A related requirement for this key internal audit competency is the analysis of the test results. Once an internal auditor has selected a sample and performed an internal audit test, the results should be analyzed. Having performed a sample per the established audit objectives, an internal auditor should review results for any possible errors detected in the sample to determine whether they are actually errors and, if appropriate, the nature and cause of the errors. For those that are assessed as errors, the errors should be projected as appropriate to the population, if a statistically based sampling method is used. Any possible errors detected in the sample should be reviewed to determine whether they actually are errors. Internal auditors should consider the qualitative aspects of the errors, including the nature and cause of the errors and their possible effect on other phases of the audit. Internal auditors should also realize that errors that are the result of the breakdown of an information technology (IT) process ordinarily have wider implications for error rates than human error.

Internal auditors should always take care to analyze and document their test sample results. They should devote every effort to making sure that the test results are representative of the overall population of items reviewed. When audit results just do not "smell" right, as sometimes happens, an internal auditor should take any follow-up procedures as necessary. However, the process of establishing audit objectives, pulling a sample of items of interest to ascertain if audit objectives are being met, and then reporting these results is a key internal audit internal audit competency.

13.5 Internal Auditor Documentation Skills

Internal auditors have a major challenge in preparing meaningful and helpful documentation covering all of their work, whether informal notes from a meeting, to audit workpapers, to the final issued audit report. Internal auditors have an ongoing need to develop strong audit work documentation skills. The next section discusses documenting results in workpapers, and Chapters 16 and 17, respectively, discuss developing effective workpapers and internal audit reports. In our electronic world of powerful word processing and database systems, that documentation sometimes can get out of hand.

Perhaps every internal auditor has received a documentation-oriented word processing message, describing some area of audit interest with some supporting message attached. Documentation becomes a challenge when that first supporting attachment has its own attachments, several of which have even more attachments, and on and on. Perhaps this type of a stream of attached documents provides the necessary and supporting information, but all too often such trails of attachments lead to ambiguities and problems. An internal audit function should establish some best practice standards for its own internal electronic documentation. In some cases, the major office automation software tools—such as Microsoft Office—will make this easy, but in other situations, there is a need to work around vendor-supplied software. For example, Microsoft's Excel spreadsheet package currently does not have a strong revision control facility, and internal auditors often need to establish their own revision control processes.

Exhibit 13.3 describes some internal audit e-office documentation best practices. We are using the term *e-office* to refer to the many word processing, spreadsheet, e-mail, and other forms of electronic documentation that an internal audit function

EXHIBIT 13.3 Internal Audit e-Office Documentation Best Practices

A substantial amount of internal audit supporting documentation and other activities takes place on computer systems, whether auditor laptops, desktop machines tied to an audit office local area network (LAN), or even on terminals connected to a central server processor. All of these comprise the e-Office—the use of email, word processing, spreadsheet, database, graphics, and other tools. The following are some best practices that internal audit should consider when implementing an effective internal audit e-office:

- **Establish hardware and software standards.** Whether internal audit is located in a more remote, developing country regions or at corporate headquarters, all members of internal audit should use the same general hardware and software product suite.
- **Use password-based security rules with regular updates.** Because of the sensitive information that internal audit encounters, password controls, with requirements for frequent changes, should implemented on all systems—even auditor personal laptops.
- **Build a security awareness.** All members of the audit team should be instructed in the sensitive nature of audit documents. For example, when documents are printed on a remote office printer, establish rules that the initiator must be present during the printing process. Even better, avoid printing internal audit documents at a remote location.
- **Backup, backup and backup.** Strong procedures should be established for at least 100% daily backups of internal audit file folders. A rotating stream of several cycles of backups should be established.
- **Establish fil revision control procedures.** Through the use of file naming conventions or software system controls, conventions should be established to identify all documents with a date created and revision number.
- **Build templates and establish style protocols.** All memos, audit programs, audit plans, and other key internal audit documents should be required to use the same common formats.
- **Establish e-mail style rules.** While there are many needs and requirements for email messages, some general style rules should be established. In addition, define and recognize areas that should be released as controlled documents rather than e-mail messages subject to forwarding.
- **Establish e-mail attachment rules.** Attached documents are an easy way to convey information, but the process can get out of hand with attachments attached to attachments and so on. Guidance rules should be established here.
- **Actively implement and monitor antivirus and f rewall tools.** Effective software should be installed, regularly updated, and violations monitored, as appropriate.
- **Limit personal use.** Whether a laptop brought to the auditor's home, downloaded music files, or a night school paper written in the office, personal use of e-office resources should be limited, if not prohibited.
- **Establish locks and security rules for portable machines.** All auditor laptop machines should be configured with locking devices as well as guidance in their use. In addition, security audit guidance should be established for all portable machines.
- **Monitor compliance.** A member of the internal audit team should periodically review and monitor compliance with auditor e-office procedures. Process and performance improvements should be installed as appropriate.

will need to support its internal audit work beyond formal workpaper binders and issued audit reports both within the audit office and for auditor laptop systems. Whenever possible, these standards should be consistent with IT department standards, but the objective should always be to support the overall internal audit effort. If all members of the internal audit team use standard practices, such as Word document revision controls, internal audit will have a greater success in controlling its

EXHIBIT 13.4 Internal Audit Documentation Best Practices

Best practices for increasing the quality of internal audit documentation:

- Writing Narratives and Descriptions
  - Describe all work in a narrative fashion such that an outsider can review some materials here and understand the activities or processes.
  - Document the audit concepts observed or performed but do not describe assumptions or speculative ideas.
  - Generate systems-related documentation with use of hyperlinks where appropriate.
- Simplification
  - Keep documentation just simple enough but not too simple—this is often an internal audit challenge.
  - Write the fewest documents with least overlap.
  - Put information in the most appropriate places—that is, allow the reader quickly to grasp the main elements of a documentation package without having to go through multiple addendums.
  - Display key information publicly by including summaries and brief descriptions where appropriate.
  - Use a whiteboard, corkboard, or internal Web site—whatever is necessary to promote the transfer of information and thus communication.
- Determining What to Document
  - Document with a purpose. For example, documentation describing test results will have a whole different focus and content from material designed for the audit staff.
  - Focus on the needs of the actual intended users(s) of the documentation who would determine its sufficiency.
- Determining When to Document
  - Iterate, iterate, iterate. Take evolutionary (iterative and incremental) approaches to gain feedback for materials under.
  - Find better ways to communicate, recognizing that documentation supports knowledge transfer but it is only one of several options available.
  - Keep documentation current. Materials that are not kept up to date are of little value to most users.
  - Update documentation regularly but only when it hurts. That is, documentation preparation resources must be balanced with other key internal audit activities.
- General
  - Always recognize that documentation is a requirement. It should not be postponed as a "when time is available" activity.
  - Require users to justify documentation requests. Check-out and back-in processes should be established.
  - Build a recognition throughout internal audit of the need for strong supporting documentation.
  - Provide documentation preparation training to all members of the internal audit team.

own automation processes. As we have stressed several times in other chapters, internal audit standards in such areas as office documentation should try to be at least as good as if not better than their enterprise's overall standards.

Going beyond our comments about effective internal audit e-documentation, all internal auditors should develop strong skills and competencies in documenting every aspect of their work. Exhibit 13.4 contains some best practice standards for documentation. Internal auditors should always keep in mind that their documentation, at all levels, may be subject to other reviews or disclosures. Whether it is a request

from an audit committee member, external auditors, court order, or even government action, poorly prepared or inaccurate documentation could embarrass or even endanger the enterprise and professionally damage both the internal audit function and the individual internal auditor.

13.6 Recommending Results and Corrective Actions

A very important role—perhaps the most important—of an internal auditor is reporting the results of audit work and developing and making strong recommendations for corrective actions, as appropriate. Internal auditors go through this exercise via their audit reports, as discussed in Chapter 17, or when serving as enterprise internal consultants, as discussed in Chapter 28. In all cases, internal auditors need to have the key skills to summarize the results of audit work, to discuss what was wrong, and to develop some recommendations for effective corrective action.

While audit reports and their recommendations are often the responsibility only of senior, in-charge internal auditors or the chief audit executive, all members of the audit team should be able to describe an audit finding and to make a recommendation for improvement. In some cases, a staff auditor will go through this exercise only as part of a workpaper note, but all internal auditors should think of much of their audit work in terms of these questions:

- What were the objectives of this audit or exercise?
- What was found?
- Why were those audit findings incorrect or not in compliance?
- What can be done to correct this error or control breakdown?
- What are internal audit's recommendations for corrective action?

This process is very much part of internal auditing. Internal auditors at all levels should develop competencies to think of much of their work along those lines. Of course, it is always important for internal auditors to answer these questions clearly and simply enough that recipients can understand the issue and the nature of the suggested corrective action. Reviewing evidence and making appropriate audit recommendations can become particularly difficult if the audit finding covers a complex or potentially obscure area. For example, many people will find it difficult to understand an audit finding describing an internal control weakness caused by an incorrect setting in an IT operating system software library. Using analogies or other mechanisms, internal auditors should strive to prepare findings and recommendations in a manner that they can be easily understood.

13.7 Internal Auditor Communication Skills

The preparation of effective internal audit reports, with meaningful findings and recommendations, is a very important competency area for all internal auditors. Internal auditors at all levels should develop the skills to discuss and present audit findings and the related internal audit recommendations. These communications can take place in the workplace at all levels.

Internal auditors typically receive, review, and have access to a large amount of potentially confidential information. For that reason, it is very important that

strong security controls be placed over all internal audit files and any retained data. However, internal auditors at all levels should develop the skills and ability to communicate with others in the enterprise about their work as appropriate and to help others to understand the value of internal auditing.

These comments are based on this author's experience with some totally non-communicative internal audit functions in recent years. In several IT consulting assignments, we encountered internal audit functions that were properly located in secure facilities but audit staff members had had essentially no contact with other enterprise members. The internal auditors, in both cases, checked into the office, went to their internal audit office area, closed doors, and were not seen until the end of the workday. Other members of those enterprises were not at all impressed with this total lack of communication.

Whether presenting the results of an internal audit to local management or dealing with others on a day-to-day basis, all internal auditors should develop strong communication skills. This is another internal audit key competency.

13.8 Internal Auditor Negotiation Skills

Whether it concerns recommendations developed in an audit report or while reviewing audit evidence on the shop floor, internal auditors will encounter many areas where management and others will disagree with their assumptions or potential findings. Auditors should beware of appearing to have an I'm-right-because-I'm-the-auditor type of attitude. Internal auditors often encounter differences of opinion during a review; auditors can sometimes be wrong, but they always need to have the background and support to explain a proposed audit finding.

Negotiation is something that we do all the time, not only for business or internal audit purposes. For example, we use negotiation in our social lives when deciding a time to meet or where to go on a rainy day. Negotiation is usually as a compromise method to settle an argument or issue. Internal auditors should communicate in order to negotiate issues/arguments, whether it is face to face, on the telephone, or in writing. However, internal auditors at all levels should recognize that negotiation is not always between two people: It can involve an internal auditor with multiple members of an auditee group.

Internal auditors at all levels should learn negotiation skills as they complete audit reports and prepare recommendations. Internal auditors should recognize that any type of audit finding, no matter how seemingly inconsequential, may be viewed as a criticism by auditee management. Sometimes an internal auditor will encounter a situation where auditee management wants to fight internal audit on every point, no matter how trivial or how solid the audit finding. Internal auditors should develop skills to negotiate and compromise on some items or areas but should always reserve the right to say that something is wrong and needs to be reported. If the auditee disagrees, it can be covered in the responses to the audit report and interactions with the audit committee if necessary.

Exhibit 13.5 outlines some elements of the negotiating process. Although this exhibit describes the overall negotiation process in a very general manner, internal auditors should keep these processes in mind when reviewing any disputed audit finding and its recommendations. Many of the points in this exhibit describe the kinds of issues that internal auditors should have in mind when presenting a draft audit report and wrapping things up. That is, even though internal auditors expect

EXHIBIT 13.5 Key Elements of the Negotiating Process

Phase I: Beginning the Negotiation—Prebargaining

1. **Information.** Learn as much as you can about the audit issue or problem to be discussed. What information do you need from the other side?
2. **Leverage Evaluation.** Evaluate your leverage or relative negotiating power and the other party's leverage at the outset. This is important because there may be a number of things you can do to improve your leverage or diminish the leverage of the other side. What will you do to enhance your leverage?
3. **Analysis.** What are the issues? This is particularly important when beginning a review of what might be a contentious audit report.
4. **Rapport.** Establish rapport with the auditee and your opponent(s). Internal audit needs to determine early on if opponents are going to be cooperative; if not, consider employing a senior member of management as a possible mediator as soon as practical.
5. **Goals and expectations.** Goals are one thing; expectations are something else. What does internal audit expect to get out of the session?
6. **Type of negotiation.** What type of negotiation do you expect? Will this be highly competitive, cooperative, or something unusual? Will you be negotiating face to face, by fax, through a mediator, or in some other manner?
7. **Budget.** Every negotiation has its costs. Internal audit may have to divert staff and management time that it could be spending on other audit efforts to meet and negotiate. Unless you are willing to allocate unlimited time and resources, you will have to make some hard choices, which should be designed to give you the most bang for your buck.
8. **Plan.** Develop a tentative negotiation plan.

Phase II: Bargaining Phase

1. **Logistics.** When, where, and how will you negotiate? This can be especially important when multiple units or locations are involved in the process.
2. **Opening offers.** What is the best offer you can justify? For example, should you modify or throw out one of several disputed audit recommendations? Should you make it, or wait to let another party go first?
3. **Subsequent offers.** How should you adjust your negotiating plan when responding to unanticipated moves by your opponent?
4. **Tactics.** What sort of tactics will you employ? What sort of tactics is your opponent using on you?
5. **Concessions.** What concessions will you make? How will you make them?
6. **Resolution.** What is the best way to resolve the problem? Is there an elegant solution? Be on constant lookout for compromise and creative solutions.

Phase III: Closure Phase

1. **Logistics.** How and when will you close the negotiation meeting? At this meeting, or later on when internal audit presents a revised draft document?
2. **Documentation.** Prepare detailed documentation describing the session, with an emphasis on planned changes and agreements by both parties.
3. **Emotional closure.** In wrapping up a meeting, it is important to address the underlying interests and needs of the parties. If you neglect the latter, the agreement will probably not last.
4. **Implementation.** Whether internal audit agrees to make some changes in a draft audit report and the auditee agrees to change some disputed practice, the negotiated agreement is of little value unless matters are implemented promptly.

agreement with a recommendation, they should go into a closing meeting fully understanding possible objections and why they are making their recommendations. As a cautionary note, when an internal auditor agrees to modify a suggested recommendation or even drop an audit finding, the matter should always be documented in as much detail as possible and with an emphasis on why the internal auditor decided to change the disputed matter.

13.9 Internal Auditor Commitment to Learning

A very significant internal auditor key competency that all internal auditors should develop is a strong commitment to learning beyond the 40 hours continuing education requirement for certified internal auditors as outlined in Chapter 27. Business and technology are always changing, as are the political and regulatory climates in which enterprises operate. All internal auditors should embrace this commitment to constant and ongoing learning as a very key competency.

The topics in many of the chapters of this book should help expand an internal auditor's commitment to learning. Two examples may explain this. Chapter 18, "IT General Controls and ITIL Best Practices," contains many areas where an internal auditor can dig a bit deeper in a pursuit of learning. While many internal auditors understand the importance of IT general controls, the information technology infrastructure library (ITIL) best practices have not been a common area of interest among internal auditors, let alone IT functions in the United States. The chapter describes ITIL on a high level and why it is important from an IT internal controls perspective. Similarly, Chapter 33 introduces the international financial reporting standards that are becoming a substitute for the U.S.-based generally accepted accounting principles (GAAP). International standards have been growing in acceptance around the world, country by country and region by region, with the United States as the only major holdout. In 2008, the Securities and Exchange Commission set rules for a conversion from GAAP to these international standards. Chapter 33 gives a very high-level overview of these international standards. Although many internal auditors will not need to understand the details of many of these accounting standards rules, they should understand their high-level impact on the reporting of financial results in the United States.

13.10 Importance of Internal Auditor Core Competencies

This chapter has introduced some key internal auditor competencies beyond internal audit standards for planning and performing effective internal audits. These are CBOK areas that all internal auditors will need to operate successfully.

These competencies are essential to all internal auditors. While topics such as good communication skills or a commitment to learning are less knowledge areas than just good practices, a strong familiarity and use of the key internal audit competencies discussed here should be required elements of every internal auditor's CBOK.

CHAPTER 14

Understanding Project Management

Project management is an important skill for many enterprise professionals, whether a marketing group launching a new product, the information technology (IT) team implementing a new application, or senior management organizing a business unit divesture. Each of these and many other efforts require detailed work activities that usually are performed as individual projects by multiple resources and under tight time constraints. No matter what their objectives and requirements, many enterprise projects need to follow strong project management discipline and approaches. Internal audit will find benefit in using good project management discipline. Although individual audits and annual audit plans have the characteristics of formal and well-managed projects, many internal auditors do not use formal project management approaches in their planning and organizing of internal audits.

This chapter looks at project management best practices and discusses why they are important tools for planning and performing all levels of internal audits. A project-based internal audit approach will generally improve internal audit's management and performance processes. While other chapters describe a body of knowledge specific for internal auditors—the common body of knowledge (CBOK)—this chapter introduces the body of knowledge of the Project Management Institute (www.pmi.org) and discusses why its concepts are also important for internal auditors. Whether at a staff level and planning individual internal audits or planning for more major audit activities, good project management techniques should improve the internal audit function. Project management skills should be part of every internal auditor's CBOK.

14.1 Project Management Processes

In past years, the term *project* often was used loosely. Internal auditors talked about their reviews as "audits," not as projects. People in other areas of the enterprise would be asked to organize a "project" to implement some special effort, and the organization and planning efforts for such a "project" meant different things to different people. Those efforts often involved a designated lead person calling the project team together and informally organizing the enterprise's planning, resource needs, and time requirements. These informal efforts often failed because the project team did not understand their individual as well as overall objectives, and neither time requirements nor project scope was defined. There often were project time and budget overruns, or projects failed for many other reasons. Often that failure was based on the lack of a consistent structured project management approach.

Several project-related definitions are important here. Project managers often use the term *program* when discussing multiple projects. A program usually is a senior-level project used to manage or control a series of related or connected projects. For example, an enterprise may want to implement some fairly large initiative that is divided into a series of separate projects. Each of the projects can operate independently, but a program structure will manage all of them together. This chapter generally refers to a project as one single effort and a program as a group of multiple related projects. An annual internal audit plan, consisting of multiple planned internal audits, can be called the annual program of planned audits for a period.

Historically, project management had been a poorly defined concept. Except for some U.S. government–led approaches, there was no consistent approach to project management. Matters changed in mid-1990, when the Project Management Institute (PMI), a project management professional organization based in Pennsylvania, was launched by a small group of U.S. professionals looking for a more consistent definition of their work. As of 2008, PMI is an international professional organization of over 260,000 members in 170 countries. PMI has researched, developed, and published a wide range of project management guidance materials. Its most significant publication is a standards-like document called the *Project Management Book of Knowledge* (*PMBOK*),[1] a comprehensive guide to all aspects of the project management process. Although not published as a government rules–type document, *PMBOK* has become the worldwide professional standard for project management practices.

In addition to the *PMBOK* guidance covering individual projects, PMI has guidance for program and portfolio management as well as the third version of its maturity model standard for *Organization Project Management* (*OPM3*). *Program management* generally refers to a series of related projects; *portfolio management* covers standards for a suite of projects and programs within an enterprise. The concepts of *OPM3* can be useful for organizing and managing an internal audit function and are discussed later in this chapter.

PMI also has a professional project manager certification program; those who complete a professional examination and satisfy experience requirements are certified as a PMP (project management professional). PMI and its *PMBOK* guide are de facto standards for many. There is also the Netherlands-based project management association called the International Project Management Association (IPMA; www.IPMA.ch). IPMA is an organization of individual country project management associations; the U.S. member enterprise is called the American Society for the Advancement of Project Management. IPMA has a four-level certification process. Candidates at each level must demonstrate their competencies through examinations and even interviews. IPMA's focus appears to be on very large-scale building construction projects, such as planning for the 2008 Beijing Olympics. This chapter focuses on PMI materials; IPMA competency approaches are introduced only briefly.

(a) Project Management Book of Knowledge

A search for books on project management in sources will yield thousands of titles, covering all aspects and variations of project management. The better ones, however, are based on the *PMBOK,* the de facto standard describing all aspects of project management. The next sections provide an overview of the *PMBOK* project management process with an emphasis on how it can be useful for managing internal

audit functions. Overall internal audit competencies should improve when these principles of good project management are followed.

At the present time, there have been three revisions to *PMBOK,* with each new set of guidance materials building on the previous versions. The current *PMBOK* version 3 defines the project management as consisting of five basic process groups and nine knowledge areas that are the elements of almost all projects. These five basic project management process groups are:

1. **Initiating.** There should be formal processes in place to launch any project effort, including a description of the project's objectives, estimated budgeting, and appropriate approvals. From an internal audit perspective, these initiating processes are discussed in Chapter 7 on launching effective internal audits.
2. **Planning.** Every project requires planning in terms of its time and resource estimates as well as for the linkages between components and other projects that require coordination. Chapter 13 on risk-based audit planning provides insights here.
3. **Executing.** These are the actual project activities—what needs to be done to accomplish project goals. From an internal audit perspective, these activities may range from individual reviews to executing an ongoing program of internal audit activities.
4. **Controlling.** An ongoing set of processes should be in place to monitor the appropriate completion of project elements, determining that budgets and objectives are being met. This can be an important component in overall internal audit management.
5. **Closing.** The final process requires wrapping up the project effort, delivering the project components as well as summarizing and reporting the project results. For many internal audit activities, the closing consists of producing internal audit reports, discussed in Chapter 17.

PMBOK matches each of these five project management processes with nine project management knowledge areas and defines each in terms of inputs, outputs, tools and techniques. For example, project inputs include the documents, plans, and necessary resources to complete a project. A wide range of tools and mechanisms are necessary to go from the starting project inputs to the completed end product. A project to build a house, for example, would need lumber, a plan, and other supplies, such as nails and roofing materials as the inputs. A hammer and a saw as well as a knowledge of carpentry are the tools necessary to get started on the construction. The output in this simplified example is the completed house.

Likewise, the launch of an internal audit project includes a set of key components, including a plan to conduct the audit, access to documentation and other materials to gain an understanding of the areas of concern, tools such as laptop systems to perform the audit, and knowledgeable internal auditors to perform the review. The construction of a single-residence frame house is a relatively small and simple project compared to many internal audit efforts. Most projects launched by enterprises of any type are complex, and this complexity is what has led to PMI and its *PMBOK* best practices standards. Often enterprises have launched major project efforts that lacked appropriate planning and resources. Many times the results were massive cost and time overruns as well as failures to complete the project. As discussed in Chapter 19, past IT new systems implementation projects were classic

examples of poor project management techniques. Massive amounts of resources often were expended, and the final project results were often late, over budget, and missed original objectives. Many other non-IT projects had the same enterprise problems. All lacked consistent and thorough project management approaches.

PMBOK has defined the project management process in a consistent and well-controlled manner. In addition to the five basic project management process groups just discussed, *PMBOK* defines nine project management knowledge areas:

1. Project integration management
2. Project scope management
3. Project time management
4. Project cost management
5. Project quality management
6. Project human resource management
7. Project communications management
8. Project risk management
9. Project procurement management

PMBOK guidance describes each of these nine knowledge areas—in terms of inputs, tools, and outputs—in a considerable level of detail. For example, *PMBOK*'s project time management knowledge area description includes input, tools, and output sections on:

- **Definin project activities.** This is the process of identifying the specific actions to be performed to produce project deliverables.
- **Sequence project activities.** The relationships between project activities should be identified and documented.
- **Estimate activity resources.** Estimates should be made for the type and quantities people, materials, equipment, and supplies required to perform scheduled activities.
- **Estimate activity durations.** There is a need to analyze activity sequences, durations, resource requirements, and schedule restraints to create project schedules.
- **Develop project schedules.** A process is necessary to monitor project status, to update their progress, and to manage any schedule changes.

These are the basic guidance steps to manage the time requirements for any project, and these are the steps an internal auditor should consider when planning the time requirements for any internal audit.

In addition to guidance on general management, *PMBOK* contains a fair degree of detail on the detailed tools and processes needed in each of these knowledge areas. Exhibit 14.1 summarizes these *PMBOK* processes and knowledge areas. The purpose of this chapter is not to provide a detailed overview of all of *PMBOK*'s process and knowledge areas but to emphasize the role of *PMBOK* for planning and implementing effective project management processes for internal auditors.

Chapter 3 discussed how, before the Committee of Sponsoring Organizations (COSO) internal control framework was launched, there was no consistent definition of internal control in enterprises nor was there a regular process for defining and monitoring those internal controls. The launch of the COSO internal control

EXHIBIT 14.1 *PMBOK* Process Groups and Knowledge Areas Summary

	Project Management Process Groups				
Knowledge Area	Initiating Process Group	Planning Process Group	Executing Process Group	Monitoring and Controlling Process Group	Closing Process Group
4 Project Integration Management	4.1 Develop Project Charter	4.2 Develop Project Management Plan	4.3 Direct & Manage Project Execution	4.4 Monitor and Control Proj. Work 4.5 Perform Integrated Change Control	4.6 Close Project or Phase
5 Project Scope Management		5.1 Collect Requirements 5.2 Define Scope 5.3 Create Work Breakdown Struct.		5.4 Verify Scope 5.5 Control Scope	
6 Project Time Management		6.1 Define Activities 6.2 Estimate Resources 6.3 Estimate Activity Resources 6.4 Estimate Durations 6.5 Develop Schedule		6.6 Control Schedule	
7 Project Cost Management		7.1 Estimate Costs 7.2 Determine Budget		7.3 Control Costs	
8 Project Quality Management		8.1 Plan Quality	8.2 Perform Quality Assurance	8.3 Perform Quality Control	
9 Project Human Resources Management		9.1 Develop Human Resources Plan	9.2 Acquire Project Team 9.3 Develop Project Team 9.4 Manage Project Team		
10 Project Communication Management		10.2 Plan Communications	10.3 Distribute Information 10.4 Manage Stakeholder Expectations	10.5 Report Performance	
11 Project Risk Management		11.1 Plan Risk Management 11.2 Identify Risks 11.3 Perform Quantitative Risk Analysis 11.4 Qualitative Risk Analysis		11.6 Monitor and Control Risks	
12 Project Procurement Management		12.1 Plan Procurements	12.2 Conduct Requirements	12.3 Administer Procurements	12.4 Close Procurements

framework in September 1992 as well as its required use in the Sarbanes-Oxley (SOx) Section 404 internal control standards has defined the standards for virtually all enterprises. *PMBOK* has similarly become such a standard for the practice of project management. The International Standards Enterprise (ISO) has a draft international standard on project management, ISO 10006, that is very similar to *PMBOK* in content and structure. Other ISO standards important to internal auditors are highlighted in Chapter 30, and this approach is the basis for effective project management standards going forward.

(b) Developing a Project Management Plan

The aim of this chapter is not to provide a process-by-process description of the *PMBOK* guidance material but to describe it as a resource to help internal auditors to plan and execute their own internal audit projects. Besides being an internal audit tool, *PMBOK* knowledge allows an internal auditor reviewing project-related activities to ask if *PMBOK* principles were used to manage that project.

To provide a better explanation of how *PMBOK* is organized and how it can become a tool to help internal auditors, we have selected an example *PMBOK* element, 4.2, on developing a project plan. While *PMBOK* is more oriented to the IT developer or manufacturing product developer, these concepts can apply to an internal auditor as well. *PMBOK* describes this project plan development area as "the process of documenting the actions necessary to define, prepare, integrate, and coordinate all subsidiary plans." Guidance here covers multiple plan areas, but internal auditors should think of this as preliminary guidance for building an internal audit plan. For example, assume that enterprise management has just acquired a company that will be folded into their main operations. While the acquisition would have taken place only before there had been some due diligence work to gain a high-level understanding of the proposed acquisition, assume that management has requested that internal audit perform a detailed internal controls review of the new subsidiary acquisition.

Every *PMBOK* element is described in terms of its inputs, outputs, and tools and techniques for that process area. Exhibit 14.1 shows that number 4.3, Developing a Project Management Plan, is at the intersection of the Project Integration Management knowledge area and the Planning Process group. Again thinking of this detailed internal controls review of the new subsidiary acquisition example, the required inputs for this process, following *PMBOK* numbering, are:

4.2.1 Project Charter. *PMBOK* emphasizes the importance of a project charter similar to internal audit charters discussed in Chapter 12.

4.2.2 Project Scope Statement. This is a key document in the audit planning process, as discussed in Chapter 15. The internal audit team launching any review needs to have a strong understanding of the audit scope.

4.2.3 Outputs from Planning Process. This step is less of an issue because internal audit goes into audit engagements with plans to document the processes reviewed as well as to deliver an appropriate audit report.

4.2.4 Enterprise Environment Factors. These factors are *PMBOK* terms that include such areas as supporting information systems, any facilities issues, or any applicable governmental standards. Internal audit should gain knowledge of these input factors and should factor them into the internal audit planning as applicable.

4.2.5 Organizational Process Assets. These include any other factors that can influence this audit plan. In this example, internal audit would use the results of the prior due diligence review as well as any internal audit work available from the prior, preacquisition internal auditors.

The project management plan is the single output from this process step. In our internal audit context, this would be an approved plan to initiate the internal audit. *PMBOK*'s tools and techniques section calls only for the need for "expert judgment" here. In our context, such judgment would be internal audit management skills to tailor processes to meet the audit's needs, to allocate necessary resources and skill levels, and to manage the audit's change management and configuration requirements.

PMBOK's Develop Project Management Plan process, as with all such elements, is not a single, freestanding process but is linked to other key *PMBOK* components. Exhibit 14.2 is a data flow diagram, adapted from the *PMBOK* guidance materials, that supports this key process and its related linkages. This exhibit shows how various *PMBOK* processes interact to develop a project management plan. For example, number 4.1, Develop the Project Charter component, is the major input to the 4.2 process. Steps 4.3 through 4.6 describe the processes to manage, monitor, and close out the project. Similar data flows could be depicted for numbers 4.1 as well as 4.3 to 4.6. Again, internal auditors should use this process guidance when planning for the steps necessary to manage, perform, and complete an audit. The activities to the right and below on the exhibit show the processes that feed the Develop Project Integration Management process; for example, there is a left-hand process on the exhibit labeled 8.1 Plan Quality. These types of internal audit quality processes are discussed in Chapter 11. *PMBOK* may seem even more complex than the three-dimensional COSO internal controls framework discussed in Chapter 3. The idea, however, is that many interconnected elements are necessary to build and maintain effective project management processes.

The *PMBOK* guidance materials discuss the inputs, outputs, and supporting tools for each of the numbered project management components, and they are all interrelated. These are standards necessary to manage any project effectively, and internal audits should think of their many of their audit activities in terms of formal *PMBOK*-type projects. While this guidance material sometimes is too broad for smaller audits, it serves as an excellent guide for managing many internal audits. *PMBOK* provides almost a checklist covering important and essential steps for planning and performing successful individual internal audits.

14.2 *PMBOK* Program and Portfolio Management

The *PMBOK* guidance focuses on individual projects and is useful for performing single internal audits. However, just as an internal audit function or department is responsible for a series of internal audits for an enterprise over a period of time, any function managing a series of projects needs to think of them in terms of a program, multiple projects as well as their relationships with other related projects. A project management program consists of a series of related projects managed in a coordinated way to obtain benefits and controls that would not be available from managing these projects separately and individually. Programs generally consist of related work that may be outside the scope of the individual projects.

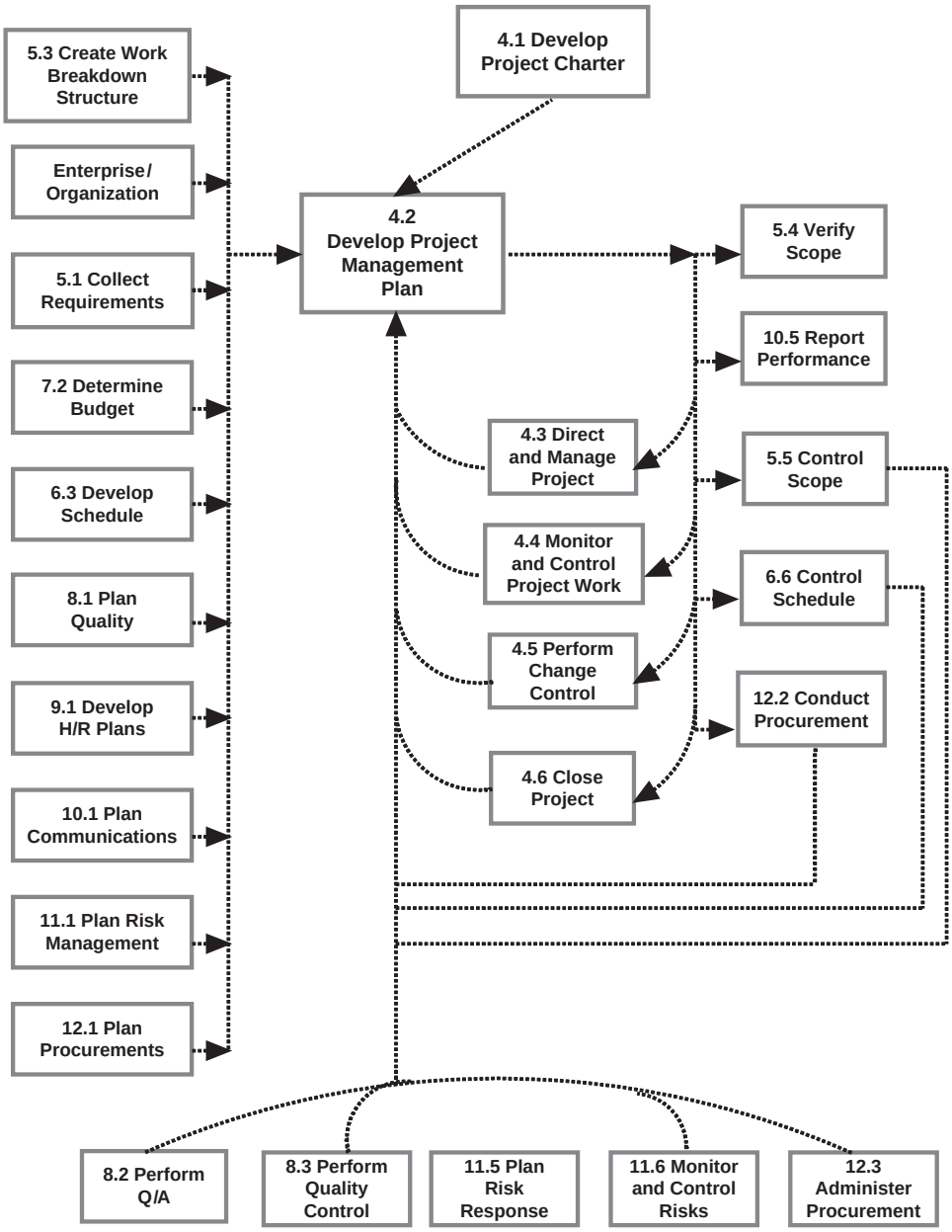


EXHIBIT 14.2 Develop Project Management Plan Data Flow Diagram

The need for program management generally occurs when an enterprise has some single objective that can be achieved only through a series of separate projects. For example, a plan to move a manufacturing facility to a new location would require a series of separate projects that all require a level of internal coordination. One project here might require moving and setting up production equipment; another would move raw materials, with still another doing IT systems conversions. Although

someone should be in charge of coordinating all of these efforts, each project will have separate needs and requirements. The projects would be managed separately but grouped together as a program.

Internal audit should think of the requirements for a series of related audit internal audit projects as a program. For example, the enterprise may be asked to review SOx Section 404 internal controls at a series of facilities. Even though each of these audits would take place at different types of facilities in different geographic locations and responsible internal audit teams, they each have similar high-level objectives, and a senior manager might be responsible for the overall completion of each. These project groups might be organized and managed as a program, with individual internal audit project managers all reporting to one program manager.

Moving up to another level, *portfolio management* refers to collections of projects, programs, and other work that are grouped together to facilitate their effective management. If internal audit groups existed for two units of a corporation, perhaps one covering internal audits in European Union countries and the other for the United States, the internal audit activities for each could be considered as an internal audit portfolio when viewed from a higher-level corporate headquarters perspective. Exhibit 14.3 describes this portfolio and program approach to project

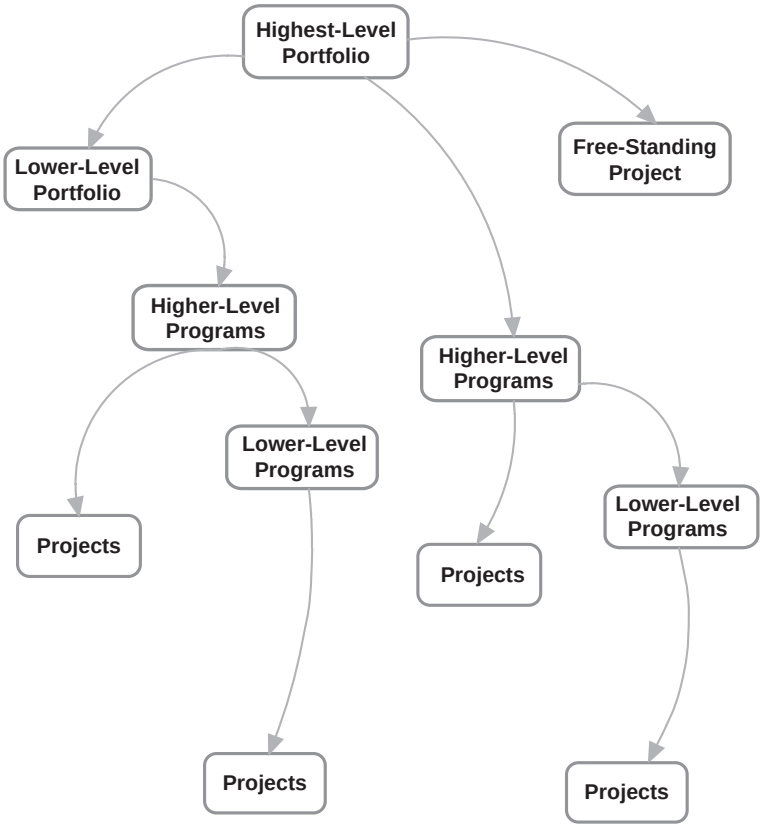


EXHIBIT 14.3 Project, Program, and Portfolio Management

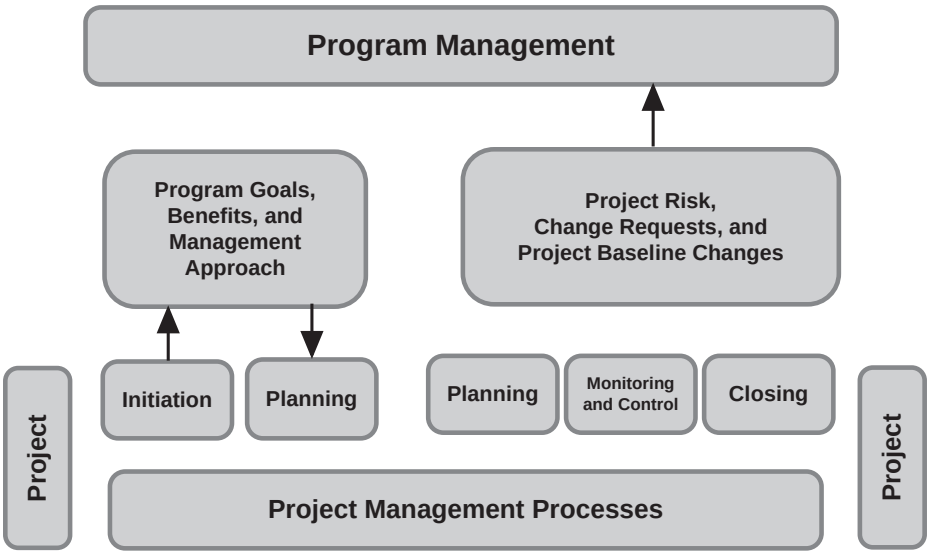


EXHIBIT 14.4 Interaction between Program and Project Management

management. The idea is that reporting relationships should be established when necessary to promote efficiency and achieve overall objectives.

PMI also has released standards for program and portfolio management, the PMI *Standard for Program Management*.[2] These are best practices for the management of multiple, related projects that are measured and evaluated as a program. PMI also has a similar but separate standard for portfolio management.[3] The guidance offered is useful to internal audit where multiple but similar projects will be managed as a program or considered as a portfolio. Exhibit 14.4 shows this interaction between the management of projects and programs. The whole idea is that there should be a tight interaction between these two. Program management does not totally drive or dictate individual project activity, and separate projects help to define the overall structure of the supporting programs. The analogy between a series of individual internal audits and the overall audit function is very strong.

The PMI program and portfolio management standards are relatively new compared to the original *PMBOK* project management guidance. Even more current is the separately published PMI portfolio management set of best practices, which takes both the project and program and program materials and defines them for high-level program management best practices. There are numerous relationships among these three. Although the PMI best practices have been tailored to a pure project management environment, internal auditors should consider PMI's best practices as a guide to managing both typical projects and internal audits.

Exhibit 14.5 shows the relationships among project, program, and portfolio management practices in terms of their scope, change management considerations, planning, management, success factors, and monitoring. Although PMI uses terms such as *project manager,* much of its guidance material is applicable to managing separate internal audits as well as either programs or portfolios of internal audits.

EXHIBIT 14.5 Project, Program, and Portfolio Management Overview

	Project	Programs	Portfolios
Scope	Projects have defined objectives. Scope is progressively elaborated throughout project life cycle.	Programs have a larger scope and provide more significant benefits.	Portfolios have a business scope that changes with strategic goals of enterprise.
Change	Project managers expect change and implement processes to keep change managed and controlled.	Program manager must expect change from both inside and outside the program and be prepared to manage it.	Portfolio managers continuously monitor changes in the broad environment.
Planning	Project managers require planning to evolve from high-level to detailed planning throughout project life cycle.	Program managers develop overall program plan and create high-level plans to guide detailed planning at component level.	Portfolio managers create and maintain necessary process and communication relative to aggregate portfolio.
Management	Project managers manage project team to meet project objectives.	Program managers manage program staff and project managers; they provide vision and overall ownership.	Portfolio managers may manage or coordinate portfolio management staff.
Success	Success is measured by product and project quality, timeliness, budget compliance, and degree of customer satisfaction.	Success is measured by degree to which program satisfies needs and benefits for which it was undertaken.	Success is measured in terms of aggregate performance of portfolio components.
Monitoring	Project managers monitor and control work of producing products, services, or results that project was undertaken to produce.	Program managers monitor progress of program components to ensure that overall program goals, schedules, budget, and benefits will be met.	Portfolio managers monitor aggregate performance and value indicators.

Source: This exhibit has been extracted or modified from the PMI best practices materials for project, program, and portfolios.

14.3 Organizational Process Maturity Model

PMBOK and the related program and portfolio management guidance are all about the concept of best practices. That, just as the *C*ontrol *ob*jectives for *i*nformation and related *T*echnology (CobiT) framework discussed in Chapter 5 and the information technology infrastructure library (ITIL) best practices in Chapter 18, these PMI materials are not "standards," where violations can make an enterprise subject

to a range of risks including even legal actions. The whole concept of best practices is particularly useful for internal auditors who typically review areas and make a range of recommendations in a wide variety of areas. As we discuss in Chapter 17, strong and effective audit recommendations often present a challenge. While it is comparatively easy for an internal auditor to find an account out of balance and to make a recommendation to fix it, internal auditors often make recommendations for improvements based on their general understandings on improving operations. No matter what the internal auditor's reputation, management often looks for some type of "authority" to support any such recommendation. A recognized set of best practices provides that support.

In addition to their project, program, and portfolio management best practices, the PMI also has released an organization project maturity model (*OPM3*) that provides an enterprise-level view of portfolio, program, and project management best practices. The best practices are designed to help an enterprise attain its strategic objectives and achieve organizational excellence in a consistent and reliable manner. A major portion of the *OPM3* material outlines a series of high-level best practices for an enterprise as well as its project, program, and portfolio management. A section of particular interest to internal auditors is the *OPM3* organizational improvement cycle.

OPM3 argues that an enterprise can realize sustainable organizational improvements through an improvement initiative based on an assessment of current practices and the implementation of a program of improvements. *Knowledge* here refers to the status of enterprise project management, its relevant maturity, and use of current use of best practices. *Assessment* consists of evaluating the status of current best practices and reviewing their capabilities. Finally, the last improvement step in the *OPM3* process calls for reviewing the material gathered and moving to a best practices environment.

This *OPM3* improvement cycle process, shown in Exhibit 14.6, should be familiar to internal auditors, as has been discussed in other audit-related chapters. The *OPM3* guidance material outlines a four-step process:

Step 1. Prepare for Assessment. This step calls for an assessment of project management maturity in relation to the published *OPM3* model. This requires gaining an understanding of the published best practices outlined in the guidance material. PMI has made this a fairly formidable task, as the published *OPM3* materials contain some 500 suggested best practices, such as #2090 for projects:

> *The organization adheres to a standard set of project management methodology, processes and procedures.*

The *OPM3* guidance material has an extensive list of best practices. An enterprise must review this list and select those practices that seem most appropriate. Although the PMI material does not provide guidance here, any internal auditor would select those best practices that are most relevant to a particular enterprise.

Step 2. Perform Assessment. Both a high-level and a comprehensive assessment are required. The *OPM3* material calls for managers to become, in

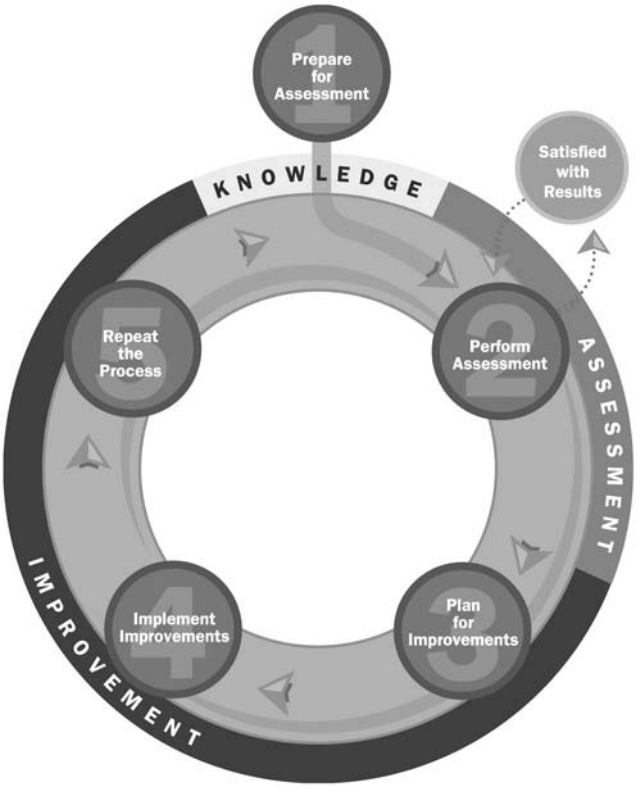


EXHIBIT 14.6 OMG Cycle

Source: Organizational Project Management Maturity Model (OPM3®). ©2003 Project Management Institute, Inc. All rights reserved.

effect, internal auditors by reviewing levels of compliance with these *OPM3* selected best practices.

Step 3. Plan for Improvements. Based on any deficiencies found in the assessment, time-based improvement plans should be developed to implement appropriate best practices.

Step 4. Implement Improvement. The improvements identified in prior steps are implemented.

Step 5. Repeat the Process. This is the same quality improvement process that should be familiar to internal auditors. Quality assurance processes are discussed in Chapter 31.

OPM3 provides somewhat of a summary to the other PMI best practices. It is relatively new and has not received much exposure, not even in enterprises that currently have strong *PMBOK*-based project management functions. We will almost certainly see some changes to *OPM3* going forward. Internal auditors performing reviews in a project management area should be aware of *OPM3* and how it is a standard to assess overall project maturity in an enterprise.

14.4 Using Project Management for Effective Internal Audit Plans

Internal auditors should think of their planned internal audits in terms of a project plan. They should perform the many aspects of that audit project following the best practices described on a high level here and found in the *PMBOK* standard. The analogies between good internal audit practices and project management are strong. Exhibit 14.1 outlined the *PMBOK*-defined project management knowledge areas. These translate to the process of planning and performing an internal audit, using *PMBOK* terminology but from an internal audit perspective, in this way:

- **Project integration management.** Detailed plans need to be prepared for every internal audit, including processes to implement changes and alter that audit plan in light of new findings or developments during the course of the audit.
- **Project scope management.** Every internal audit needs to establish and document a clear statement of the audit's scope at the beginning of the review. This scope will become a baseline for measuring internal audit progress, accomplishment of the scope's objectives, and any necessary change control.
- **Project time management.** The time and activities of all internal auditors involved in a review need to be budgeted, recorded, monitored, and assessed.
- **Project cost management.** Internal audit costs needs to be budgeted, collected, and controlled.
- **Project quality management.** Every internal audit project needs to have quality planning, assurance, and control processes. These measures assess a particular audit as well as the overall internal audit function.
- **Project human resources management.** Proper attention must be paid to the team performing the internal audit, including audit team organization planning and all levels of staff development and training.
- **Project communications management** . Communications are important elements in any internal audit, whether in documenting results in workpapers, communications to management and audit management, and development of the final audit report.
- **Project risk management** . Every internal audit faces a variety of risks. The internal audit team needs to have processes in place to formally identify and quantify these risks as well as to respond and control any risks associated with an internal audit.
- **Project procurement management** . Although they are perhaps the least significant of the *PMBOK* knowledge areas when compared to other aspects of an internal audit, procurement management processes should be in place during any audit when necessary to contract for any required outside services and goods.

14.5 Project Management Best Practices and Internal Audit

Effective project management best practices, as defined in *PMBOK,* are an important CBOK for all internal auditors, both in developing internal audit projects and in assessing the maturity of project management practices in the course of their reviews.

This chapter has provided a high-level overview of *PMBOK* and project management. Internal auditors should take steps to increase their skills and knowledge in this very important discipline. Internal auditors should use project management tools and methods as an aid for more efficient and effective internal audits.

Notes

1. Project Management Institute, *A Guide to the Project Management Book of Knowledge* (*PMBOK Guide*), 4th ed. (Newtown Square, PA: PMI Global Operations Center, 2004).
2. Project Management Institute, *The Standard for Program Management,* 2nd ed. (Newtown Square, PA: PMI Global Operations Center, 2002).
3. Ibid.

CHAPTER 15

Planning and Performing Internal Audits

Past chapters have focused on components to build an effective internal audit function in an enterprise, internal audit practice standards, and other factors for assessing an array of potential internal audit candidates in an enterprise and selecting appropriate candidates for an internal audit. Other chapters generally focus on more specialized internal audit areas, such as reviews of information technology (IT) general controls, but this chapter reviews the steps necessary to plan and perform an individual internal audit. Of course, nothing is ever typical in the vast and varied worlds of internal auditing, but this chapter uses the example company from other chapters, Global Computer Products, to describe some processes necessary for planning and launching an internal audit.

We focus on a financial/operational internal audit review of the material receiving and accounts payables functions using our example company, Global Computer Products, at its manufacturing plant. This chapter cannot cover all of the many controls risks and other aspects of such an operation, but it walks through some important characteristics of such an internal audit. Our assumption here is that the internal audit team focuses primarily on operational internal controls with less emphasis on financial issues and its supporting IT systems.

Although this chapter paints an environment that may not be typical for everyone, it goes through some common internal audit steps. The overall common body of knowledge (CBOK) theme discussed throughout this book has focused on areas where internal auditors should have a good understanding and others where they only need to have just a general understanding. This chapter walks through the steps of an actual internal audit, the basic activity of all internal auditors. All internal auditors should have a strong CBOK understanding, if not hands-on experience, in this process of planning and performing individual internal audits.

15.1 Understanding the Environment: Launching an Internal Audit

Chapter 10 talked about the importance of building an audit universe, an approved and documented description of all of the potential candidates for internal audits within an enterprise. The idea of such an audit universe document is to describe the scope of internal audit's planned activities. For example, assume our example

company has a small product manufacturing plant in the city of Muddville and has an advanced products research facility at that same location. When assembling its audit universe description, internal audit management may have decided that the Muddville advanced products facility was too small, too specialized, or otherwise out of scope for internal audit. However, we have assumed that internal audit has decided to review the Muddville plant manufacturing direct materials cycle, the internal controls covering purchasing, receiving, accounts payable, and overall accounting cycle operations. In addition, because the accounting cycle will be covered as part of Sarbanes-Oxley (SOx) review procedures and their external auditors later at year-end, our example review will focus on purchasing and receiving processes.

Although these processes were highlighted on the audit universe list, further assume that internal audit has never performed a purchasing and receiving processes review at this unit but has decided that the facility's relative growth requires some internal audit work. This situation is not unusual for many internal audit functions. A large number of potentially auditable resources will be listed on audit universe documentation, but because of the lack of time, resources, and other matters, some of these potential auditable entities never are candidates for internal audit reviews. They may remain on the back burner until growth or other issues cause management attention or until a member of senior management or the audit committee asks if internal audit has ever done any work at that facility.

In this example, assume that internal audit has decided to launch a review of the Muddville facility operations as part of an annual internal audit planning process. We assume that internal audit has established audit programs for reviews of these areas, as discussed in Chapter 10, and has enough general knowledge about operations to launch the internal audit.

An important first step in any internal audit is to look at other internal audits either in process or planned over the short term, to consider the availability of internal audit resources, and then to prepare a preliminary internal audit plan. Let us assume that the Muddville facility is out of town but will not require any long-distance international travel to visit the location. We will also assume that the chief audit executive (CAE) and other internal audit team members have sufficient knowledge of plant operations that a preliminary visit is not necessary. Based on available information, internal audit would prepare a preliminary plan for the upcoming Muddville audit.

Exhibit 15.1 is a preliminary plan that might be developed for such a review. Because the information on the exhibit is very preliminary, the plan does not show specific dates but assumes that two internal audit staff members will be assigned to do the work. The preliminary plan provides approximate estimated weekly activities. Care should be taken not to seal such preliminary plans in cement, as more information may force all planned estimates up or down.

Having developed preliminary plans for the audit, a next step is to inform the responsible management at that facility through an internal audit engagement letter. Exhibit 7.3 in Chapter 7 is an example of such an engagement letter. Usually communicated along with some high-level preliminary discussions, the engagement letter announces the planned audit along with its objectives, approximate dates, and assigned internal auditors. Because local management often claims that the audit's timing is bad or other problems, the final audit plan may have to be adjusted.

EXHIBIT 15.1 Muddville Purchasing and Receiving Preliminary Internal Audit Plan

Location: Muddville Plant Facility
Assigned Audit Team:

REF	Audit Activity	Week 1	Week 2	Week 3	Week 4	Week 5
1	Review past activity and assess risks	**X**				
2	Develop audit approach and plan	X				
3	Contact site to schedule audit	X				
4	Travel	X			X	
5	Review and document processes		X			
6	Perform walk-throughs to confirm understanding		X	X		
7	Perform tests of internal controls		X	X		
8	Perform other audit procedures per audit plan			X	X	
9	Summarize and confirm audit results				X	
10	Complete audit workpapers				X	
11	Schedule audit closing meeting				X	
12	Prepare draft audit report for corrective action					X

15.2 Documenting and Understanding the Internal Controls Environment

We stated that our example internal audit function has never performed a review of purchasing and receiving operations at its Muddville facility but that it has audit programs and experience in performing similar reviews at other Global Computer Products facilities. Because local processes and even supporting systems may differ from one plant to another, internal audit will need to gather more data and information about operations at Muddville. In an ideal world, internal audit can simply contact the local facility to be audited, ask it to send copies of flowcharts and other documentation, and go from there to begin preliminary internal audit work.

We are only describing an ideal world, however; in reality, such documentation may be sparse, out of date, or nonexistent. Internal audit may want to ask some questions to gather more information about these processes. Exhibit 15.2 is an example questionnaire that internal audit can circulate to gain information about the environment in which it plans to perform an internal audit. The results of that questionnaire should help internal audit to plan its review, including the size and types of items to sample as well as the need for any IT application control, reviews, and computer-assisted audit tools, as discussed in Chapters 19 and 21, respectively.

Effective internal audits generally cannot be performed by internal audit working in the corporate office and gathering audit evidence through e-mail messages and file queries. In almost all cases, internal auditors need to have their feet on the ground and must spend some time visiting the auditee site and observing operations. Internal auditors typically can learn a lot by spending time at a site, even if sometimes it is only the result of general impressions. On-site internal auditors should observe various activities and actions while performing the audit fieldwork: a manager who

EXHIBIT 15.2 Muddville Purchasing and Receiving Internal Audit Information Questionnaire

1. Are all material purchases authorized through formal, approved purchase orders?
2. Is purchasing based on a set of authorized, approved vendors?
3. Are approved vendors screened periodically for performance factors, such as on-time delivery, compliance to specifications, etc.?
4. Are there any monetary or quantity limits on purchase orders that require additional approvals?
5. Do all purchase orders comply with authorized payment and delivery expectation standard terms?
6. Is the approved corporate purchasing system used for all material purchases?
7. Do all material receipts go through regular receiving operations?
8. Are there limits regarding the times when receipts are accepted?
9. Are approved corporate receiving systems used for the receiving process?
10. If incoming materials do not match to a purchase order in terms of P/O documentation, quantity, approved deliver dates, or other factors, what processes are in place to resolve these issues?
11. Are all critical materials subject to inspection?
12. Are there standard documented processes in place for materials that do not match inspection criteria?
13. . . .
14. . . .
15. *And other detailed questions to allow internal audit to gain an understanding of these processes*

always arrives very late, an analyst who does not appear to be following good IT security procedures, or any of many other observations. Many may not result in formal internal audit recommendations, but they will help internal auditors to gain some overall impressions of the unit being audited. Some of these matters can be formally documented in internal audit workpapers, while others are just impressions that can be used to support the overall audit conclusions.

Far more important than just observations, internal auditors need to develop a good understanding of the materials they are reviewing, prepare documentation to support or update any existing materials, and then use that material to identify any internal controls vulnerabilities or to help in internal audit's understanding of the processes being reviewed. Chapter 16 discusses documenting results through process modeling and mentions that there are many accepted documentation approaches. Exhibit 15.3 shows a receiving function sample flowchart. The idea is to show decision points in the process that are often areas for audit tests. For example, this exhibit has decision steps on whether received material has passed an inspection test and then another whether material is sent back to a supplier.

Our aim here is not to describe a process in detail but to show how appropriate internal audit process documentation can define key decision points. In this example, if local management was concerned that bad, defective material was improperly entering into the production process, the internal auditor could use such a process flow to identify a point where, if material was not given proper inspections, bad material could enter into the production process.

Diagrams such as Exhibit 15.3 can be prepared to describe an internal auditor's understanding of processes at the facility being audited. The internal auditor needs to confirm that such a documented description is correct. Our sample flowchart

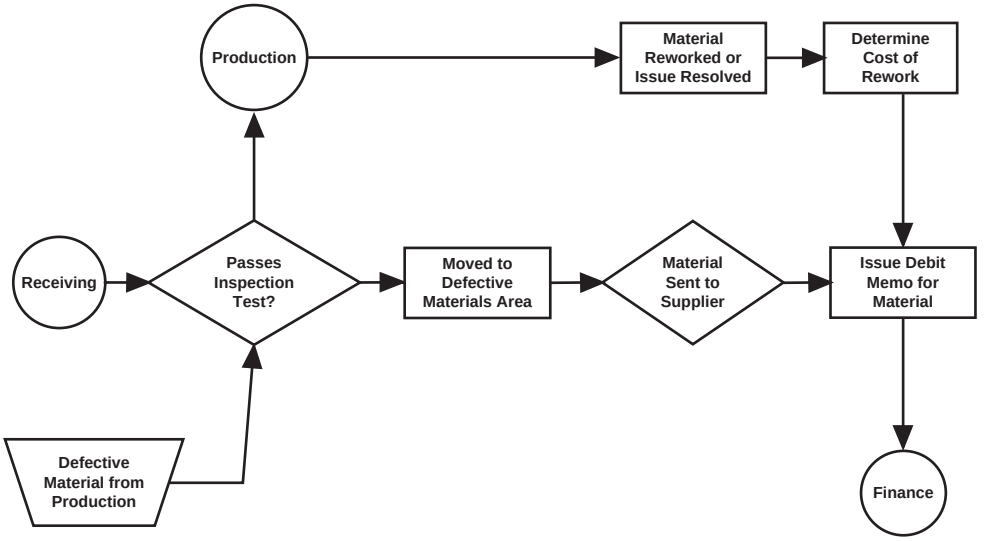


EXHIBIT 15.3 Receiving Functions Sample Flowchart

shows a relatively simple process. An internal auditor can draw such a flowchart in the area being documented to determine if the description is generally correct. Many processes and supporting flowcharts, however, are so complex that an internal auditor cannot just expect to show the flowchart to a manager on the site to ask if it is OK. Often more supporting information is needed.

A walk-through exercise is often an effective way to verify that the process documentation is correct. This type of exercise is most effective in very complex processes with many twists and turns and multiple decision points as well as multiple people-dependent decision points along the way. The idea is that an auditor would take a document, such as a material receiving report, and manually walk through each of the steps being reviewed. The internal auditor should attempt to determine that the personnel at each step in such a decision chain actually perform the process as described. Results here can sometimes be interesting. The internal auditor may present the document being analyzed to floor personnel to ask how they would process it. Sometimes the internal auditor will find that the process as documented is not working as described.

If so, in most cases, the prepared documentation needs to be revised. However, in some situations, interviews during a walk-through may identify potential internal control weaknesses. These are situations where unit management appears to think how a process should be working but an internal auditor, through interviews with people actually performing procedures, may find that actual operations are quite different. Situations like this may require some rethinking or revisiting.

15.3 Performing Appropriate Internal Audit Procedures

Assuming that the documented processes are correct and complete, internal audit next needs to identify key internal control areas and then develop audit tests to verify

that those controls are working. The size and nature of these tests depend very much on the nature and criticality of the process. However, it is usually not sufficient to select one item to walk through the process and then to say that everything is OK as long as that one item met this audit test.

Chapter 9 discussed audit sampling, including using statistical and nonstatistical procedures to sample and evaluate audit evidence. Although some aspects of statistical sampling are complex and can lead an internal auditor into troubles, that chapter recommended that all internal auditors should have at least a CBOK general understanding of statistical sampling processes. Such knowledge will allow internal auditors to state with some confidence whether internal controls appear to be working or whether an account balance is correct.

In our example audit here, the internal audit team would have arrived at the Muddville plant site, confirmed the process documentation prepared prior to arrival at the audit field site, or created documentation during the first audit steps. Next, after reaffirming that documentation through walk-throughs, internal audit needs to refine its own internal audit procedures and then perform the audit tests.

In our environment, the internal audit function may have arrived at the audit site with some established audit programs for the areas to be tested and evaluated. However, often the internal audit team on-site may need to make some small adjustments to audit programs prepared by internal audit management. In all such circumstances, the internal audit team should obtain, from internal audit management, approval for any audit program or procedure changes and then go on to perform the actual audit steps as documented.

Our example internal audit describes a relatively limited set of procedures that would be performed with a small internal audit team—here two internal auditors—and over a fairly short time duration. There are many other internal audit situations, however, where an internal audit will be much larger in terms of the areas reviewed, the size of the audit team, the time duration, and many other factors. Strong project management tools, as discussed in Chapter 14, are essential for such an extended review.

No matter what size, the internal audit team needs to develop effective internal audit workpapers, whether in traditional hardcopy files or laptop computer-based soft-copy workpapers. Both workpaper formats as well as other formats to control and better manage internal audit are discussed in Chapter 16.

15.4 Wrapping Up the Internal Audit

After the on-site internal audit team has completed its audit tests and performed other internal audit procedures, there is a need to wrap up the audit fieldwork before departing from the audit site. Although the final audit report and even a final draft report may not be complete prior to internal audit's departure, on-site internal auditors must provide local management with at least a summary of audit observations and potential findings and recommendations. Chapter 17 discusses the importance of internal audit reports, and Exhibit 17.6 summarizes the preparation steps necessary to prepare and issue effective internal audit reports.

Even though it may take some additional effort and audit resources to prepare even a draft audit report prior to the end of the audit fieldwork, internal audit should at least issue auditee management an audit findings point sheet that outlines internal

audit observations and potential recommendations. Field auditors should not to try to prepare a draft audit report before a more detailed review and approval by audit management. Although internal audit reports have always been important, SOx requirements have made them even more critical because the audit committee now will have full access to all internal audit reports. In our era of e-mail attachments, it is quite easy for a report—even one labeled "draft"—to be circulated and misinterpreted. A draft report that develops some incorrect or even embarrassing conclusions should be tightly controlled and monitored.

There are some situations, of course, where an internal audit team can leave an audit engagement with a strong draft or almost final audit report. For example, when an enterprise has a large number of small retail or restaurant locations, the internal auditors performing the review often will be doing an almost checklist compliance-type of review, looking for such matters as whether required daily documents are kept up to date. A full, final audit report makes sense in such situations.

For larger, perhaps more comprehensive internal audits, such as our Global Computer Products review of the Muddville plant facility, it is a better idea for internal audit management to review and approve even the draft report. However, an internal audit point sheet is sometimes a very effective way to document internal audit observations. This document summarizes internal audit preliminary findings along with potential recommendations. Exhibit 15.4 is an example of such a point sheet. Point sheets essentially are discussion documents. In cases where management has some significant areas of dispute, internal audit can document and agree to

EXHIBIT 15.4 Audit Fieldwork Preliminary Findings Point Sheet

Global Computer Products

Internal Audit Point Sheet

Audit: Muddville Plant Purchasing and Receiving Operations
Date: yy/mm/dddd
Internal Audit Team Lead:

Note: These comments are preliminary internal audit findings and potential recommendations as a result of the recent internal audit review. The final results will be published in a soon-to-be issued internal audit report. While the final findings and recommendations may be subject to change, internal audit recommends that operations management begin corrective action steps in advance of the formal internal audit report.

Audit Finding #1: Incoming materials are not receiving required quality inspections, per established procedures. Although procedures require detailed inspections for finished electronic subassemblies, we found that some goods are being moved directly to production operations. In a sample of 15 incoming finished subassemblies, we found that receipt had been moved directly to the production area, bypassing quality inspections.

Recommendation: . . .
Audit Finding #2: . . .

review draft findings again or to make changes to clear up any management areas of concern.

The aim of an effective internal audit is not for field auditors to come home with a dazzling audit report filled with findings and recommendations but to review an area and to make recommendations to improve the overall internal controls environment. Often internal auditors miss this objective as they get involved with "gotcha" kinds of audit findings. As we have discussed, the aim of internal auditors should always be to provide overall service to management.

15.5 Performing Internal Audits

This chapter has revisited some considerations necessary to perform individual internal audits. There are many different audit approaches to consider, and internal auditors should use many of the procedures discussed here and elsewhere. Internal audits are effective only when an internal audit team establishes audit objectives; visits the area to be audited and gathers information to document and describe internal controls; tests those controls to determine whether they are effective; and then wraps up the audit by making recommendations for controls improvements, as appropriate.

Although some members of internal audit management get involved in desk jobs away from field activities and do not perform internal audits directly, every member of an internal audit function should have a strong CBOK level of knowledge of what it takes to plan and perform effective internal audits. That is a fundamental skill requirement in the internal audit process, and every internal auditor, from CAE to audit staff members, should be familiar and comfortable with the basic internal audit process.

CHAPTER 16

Documenting Results through Process Modeling and Workpapers

Internal auditors observe many process-related problems or errors in data and operations as part of their internal audit reviews. However, management will not fully recognize those concerns and findings unless they are supported by strong supporting documentation. An internal auditor can describe a high-level internal controls concern in a summary of audit results, but if managers responsible for the area audited question the finding, they will respond with a "show me" request. Internal audits need strong documentation to support audit findings and observations. In addition to effective internal audit reports, as discussed in Chapter 17, good documentation must support the internal audit work.

The effective documentation of audit evidence is a very important internal audit skill requirement. There are two dimensions to this documentation. First, internal auditors often are exposed to a wide range of information on the business and its operations at a site. In order to better understand control strengths and weaknesses, auditors need to think of these activities in terms of their supporting processes, which often may not be adequately documented. This chapter reviews procedures for describing and documenting these activities through what is called process modeling. Some professionals use process modeling techniques that result in complex diagrams; here we explore effective process modeling for internal auditors—an important common body of knowledge (CBOK) skill.

The chapter also outlines techniques for documenting internal audit work in audit workpapers or audit evidence. These are the materials that are assembled to describe an internal audit. Audit workpapers are very important for individual internal audits and for the total enterprise. In some situations, they can even become a source of evidence in litigation. Once organized in voluminous paper-based files, today audit workpapers are best organized in digital format and assembled on laptop computers. This chapter discusses some best practices for organizing internal audit workpapers.

Internal audit has a financial reporting and legal requirement to retain its audit workpaper documentation for periods of up to seven or more years. This can be a challenge; technology changes sometimes make accessing old records difficult, and physical space limitations present a challenge to keep track of old records. The chapter concludes with a discussion of internal audit record management and

retention best practices. The describing, documenting, and maintaining records of internal audit activities are all internal audit CBOK requirements.

16.1 Internal Audit Documentation Requirements

Internal auditors spend most of their time reviewing records, performing analyses based on those records, and interviewing people at all levels in the enterprise to gain information. Auditors use all of this information to develop audit conclusions and to make appropriate recommendations. However, this effort is of little value unless the audit work is documented in an orderly manner both to support the current audit effort and provide a historical record. If internal auditors did not cover all of the details at the conclusion of a current review, they can always rely on personal memory to fill in some missing detail or observation when wrapping up and concluding an audit. However, those undocumented observations are of little value if the audit results are called into question—sometimes even for legal proceedings—months or even several years into the future. The person who did the work may have moved on, and the internal audit work cannot be corroborated. Strong, ongoing internal audit documentation is essential.

Internal audit documentation refers to published audit reports, action plans, and other materials supporting the reports, audit workpapers, key meeting minutes, computer-assisted audit tools and techniques (CAATTs) materials, and any other data and information to support an internal audit. Of course, internal audit documentation should not be retained in perpetuity, and an internal audit function should establish and follow some documentation retention minimum standards. While different countries and governmental units may have different rules, a good rule of thumb for internal audit document retention is the U.S. Securities and Exchange Commission (SEC) rules for external audit financial records.

The SEC requires that "records be retained for seven years after the auditor concludes the audit or review of the financial statements."[1] For an internal audit, the records retention period would be a minimum of seven years after the audit report is released. While public accounting firms are subject to Public Company Accounting Oversight Board rules as well as potential shareholder legal action, internal audit is not quite under the same spotlight. Nevertheless, an internal audit function should arrange to retain all significant records from an internal audit for this seven-year retention period.

The next sections discuss three important aspects of internal audit documentation: process modeling, audit workpapers, and document management. Internal auditors often begin a review in a new process area where there may have been no previous audits and even limited enterprise documentation. The internal auditors need to observe operations, review reports and procedures, and ask questions to develop an understanding of that new process. The resulting documentation is important for understanding the internal control environment and for making consulting-related recommendations when appropriate.

Workpapers are the second major topic of this chapter. These are the documents that describe an internal auditor's work and provide the basis and understanding for the internal audit. We have moved from printed and handwritten paper documents to an era where audit work is assembled on laptop computers; good documentation

security and retention procedures are critical. A basic understanding of these areas should be basic internal auditor CBOK requirements.

16.2 Process Modeling for Internal Auditors

Business process models or descriptions are maps that help an internal auditor navigate through business activities:

- Where we are right now
- Where we need to go
- Where we have come from
- How we have gotten to where we are

Process models are really a form of map to help an internal auditor navigate through a series of observed activities. However, good process modeling is more that just a simple road map showing how to get from one point to another. Such a map will not help if we make a wrong turn somewhere along the way, and we need a more detailed road map to get back to the initial intended course. Exhibit 16.1 shows a very simple process model for a custom products manufacturing process that an internal auditor has been asked to review. Here some enterprise process group receives inputs or orders from its customers and delivers the completed products to them. However, in order to produce the output, it must coordinate with suppliers, and there must be a measurement system feedback loop to promote product improvements.

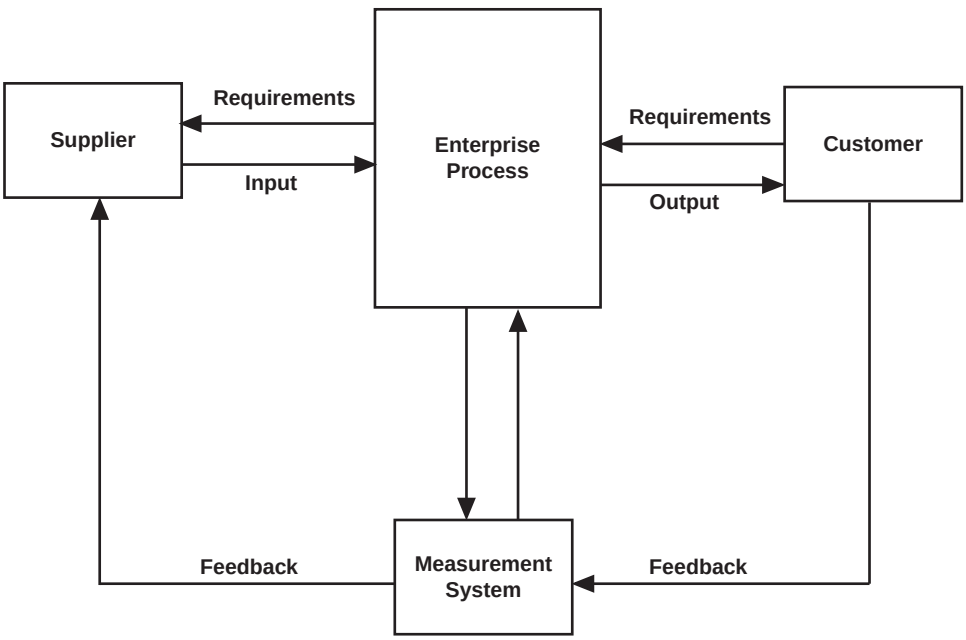


EXHIBIT 16.1 Simple Process Model

This is the type of simplified chart that an internal auditor might draft on a first visit to a facility when asking questions about its activities. Using this chart, an internal auditor can gather more detailed information, such as specific input and output requirements between the process owners, the activities that transform a suppliers input into an output that meets customer requirements, and the feedback and measurement systems that are necessary to make the process work. It is necessary to go a level or more beyond this simplified model for greater process information. For example, the operations processes could be defined in terms of planning, engineering, procurement, order entry, accounts payable, and accounts receivable detailed processes.

(a) Understanding the Process Modeling Hierarchy

Sometimes business units develop their own process charts covering key activities. Often, however, internal auditors have to spend part of an initial visit gaining an understanding of operations. Some key process definitions will help internal auditors to better communicate with others, particularly others who have been trained and understand process management concepts:

- **Systems.** Related processes that may or may not be connected.
- **Processes.** Logically interconnected, related activities that take an input, add value to it, and produce an output to another internal process or output customer.
- **Activities.** Small parts of a process that are performed by a single department or an individual.
- **Tasks.** Steps that are required to perform specific activities.
- **External customers.** Entities outside of the process supplier's unit that receive a product, service, or information from the supplier.
- **Internal customers.** Persons, departments, or processes within the enterprise that receive output from another process.

As part of understanding and describing processes, internal auditors need to understand how these process elements relate to one another. Exhibit 16.2 shows a process hierarchy breakdown for what should be a familiar process for internal auditor: elements involved in performing an internal audit. An actual process description would be much more detailed, but this exhibit shows that the evaluate internal controls process of internal audit points to a whole stream of subprocesses.

Performing a process analysis and documenting key elements requires much more effort than the preliminary auditor walk-throughs described in Chapter 7. Internal auditors will need to assemble to team of personnel involved in the process area and go through a process area in some detail, defining such things as input and output criteria, potential errors associated with each link, and feedback mechanisms to correct those errors. This process can be time intensive, but it should benefit current and future internal audits in the review area.

(b) Describing and Documenting Key Processes

Process descriptions prepared by internal auditors should be part of the audit workpapers for any review, as describing in the next section. Their purpose is to describe the flow of inputs and outputs between these process activities. They require strong

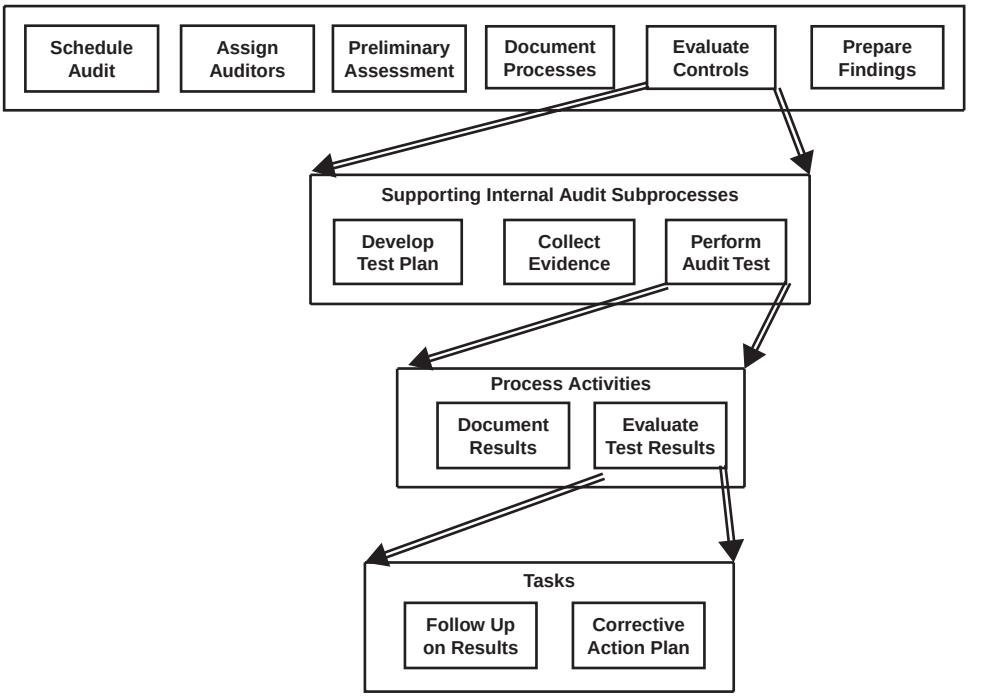


EXHIBIT 16.2 Process Hierarchy Example: Performing an Internal Audit

descriptive material as well as flowchart diagrams. Although such documentation was once prepared with pencil-and-paper methods that went out of date quickly, powerful automated tools on laptop computers develop process flowcharts easily. Many strong products are on the market; SmartDraw and Visio are excellent software products to consider. (Note that this book does not endorse one product over another.) Before acquiring graphics software, an internal auditor should meet with information technology (IT) or quality assurance managers to ascertain what software they are using.

Based on any other modeling products in place, internal audit should develop diagramming standards to use in describing their enterprise processes and internal controls. These diagramming standards consist of flowcharts and brief descriptions. The descriptions, of course, should follow the same standards that internal audit is using in all of its audit workpaper descriptions, often bulleted notes that describe an interview that the auditor has conducted as well as the documented time and date of the interview. These notes should be reviewed and approved by a supervisor and protected from any future unauthorized alterations. They are an element of the internal audit workpapers and require document retention controls.

A survey of process modeling texts will show many alternative diagramming approaches. Many are very complex and should be avoided; others place too much emphasis on describing all of the detailed decision points in a process—similar to detailed flowcharts that were once used to document a COBOL program. Internal audit must develop a standard and consistent approach for its process modeling flowcharts. Two easy-to-use and understand approaches are input/output flowcharts and work-flow charts.

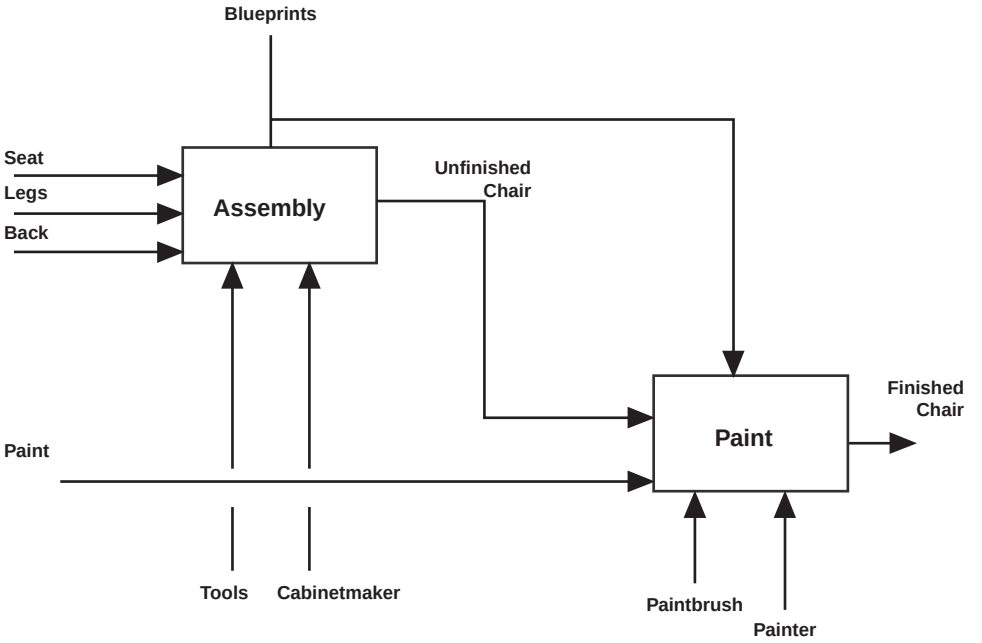


EXHIBIT 16.3 Input/Output Process Flowchart

(i) **INPUT/OUTPUT PROCESS FLOWCHARTS** The flow description approach is best for processes that deal with physical objects. Its focus is on the passive participants that are being consumed, produced, or changed by the process activities. This type of a flowchart is a road map for transporting process steps from one activity to the next. Exhibit 16.3 shows an input/output process flow for manufacturing a wooden chair. Using an established blueprint, the various part inputs are transferred to an assembly process. Once completed, the chair moves to a painting process. This is a simple diagram, but it shows how process inputs and outputs move through an operation.

(ii) **WORK-FLOW DESCRIPTION PROCESS FLOWCHARTS** A work-flow description process flowchart places its emphasis on the order of activities rather than what activity does the work. Exhibit 16.4 is an example of this type of flowchart showing a payment and shipping flow. Here all activities must be done in a specified order. For example, in the flowchart it is essential to receive payment before shipping the goods. In this type of diagram, emphasis is not on the participants but on the order that the process should flow. Because many internal audits involve office-type activities rather than manufacturing work steps, this form of process flowchart is often best to provide a road map of the types of activities that an internal auditor will encounter.

(c) Process Modeling and the Internal Auditor

Process modeling is an important internal auditor tool both for reviews of existing enterprise processes and to suggest areas for improvement. Chapter 28 discusses the

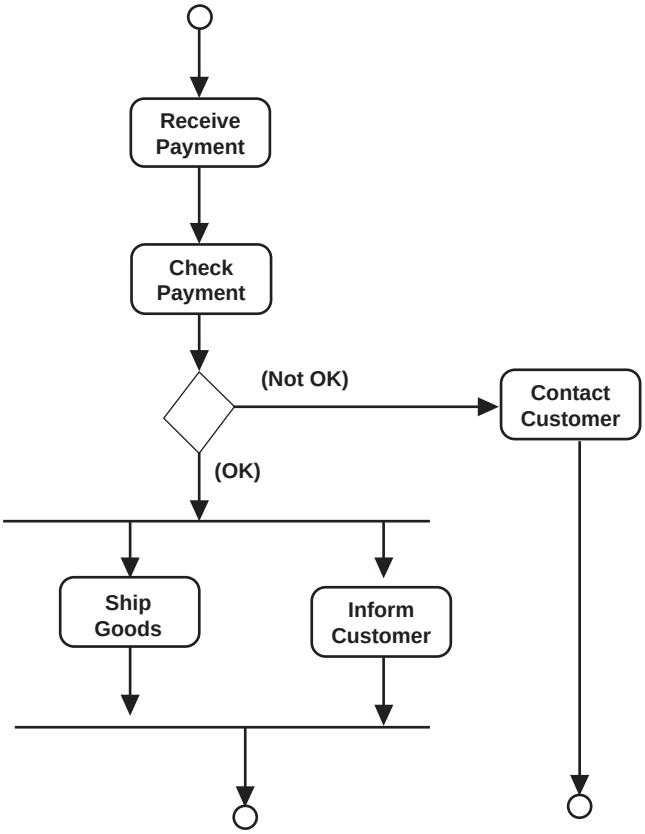


EXHIBIT 16.4 Workflow Process Flowchart

role of an internal auditor as an enterprise consultant; an understanding of process modeling tools and techniques is essential there. An auditor can meet with enterprise teams and identify areas for improvement.

This chapter contains a very high-level description of process modeling. While the work-flow type of flowchart described here is not that complex, an internal auditor may want to gather more information to increase process modeling skills. Internal auditors schooled in Institute of Internal Auditors' methods may not be experienced in process modeling techniques, but anyone involved with quality assurance processes should be familiar with them. Chapter 31 discusses quality assurance auditing and approaches. Every internal auditor should have at least a minimum level of process modeling and flowcharting knowledge.

16.3 Internal Audit Workpapers

Workpapers are the written records kept to gather documentation, reports, correspondence, and other sample materials—the evidential matter—accumulated during an internal audit. The term *workpaper* is a rather archaic auditor expression that describes a physical or computer file that includes the schedules, analyses, and

copies of documents prepared as part of an audit. Workpapers are the evidence to describe the results of the internal audit. They should be formally retained for subsequent reference and substantiation of reported audit conclusions and recommendations. As a bridge between actual internal audit procedures and the reports issued, workpapers are not an end in themselves but a means to that end. Workpapers are created to fit particular audit tasks, and their preparation may be subject to a great deal of flexibility. They must support and document the purposes and activities of an internal auditor, regardless of their specific form. Thus, workpaper principles and concepts are more important than just their specific formats.

Internal audit workpapers can also have legal significance. In some situations, they have been handed over, through court orders, to government, legal, or regulatory authorities as supporting evidence. When scrutinized by outsiders in this context, inappropriate workpaper notes or schedules can easily be taken in the wrong context. Workpapers form the documented record of who performed the audit and who reviewed the work. Internal audit workpapers are the principal record of the audit work performed, and at some time they may provide evidence of what did or did not happen in an audit.

This section provides general guidance for preparing, organizing, reviewing, and retaining workpapers. While once organized in bulky legal-size paper folders, audit workpapers today are stored as computer-based folders or a combination of paper and computer format documents. The preparation of workpapers is a basic internal auditor CBOK requirement. As a side note, this and other chapters use the term *workpaper*. Readers may also see *working paper* or *work paper*. All mean the same thing.

As discussed in previous chapters, internal auditing is an objective-directed process of reviewing selected business documentation as well as interviewing members of the enterprise to gather information about an activity to support the audit objective. The internal auditor then evaluates these materials and information gathered from interviews to determine if the objectives of the audit are being met and whether appropriate standards and procedures are being followed. Based on this examination, the auditor forms an audit conclusion and opinion that is reported to management, usually in the form of audit findings and recommendations published in an internal audit report, as discussed in Chapter 17. An internal auditor, however, should not just casually flip through some reports or observe operations to give management impressions of what was found. The audit evidence, documented in the auditor's workpapers, must be sufficient to support the auditor's assertions and conclusions.

The overall objective of workpapers is to document that an adequate audit was conducted following professional standards. The major functions of auditor workpapers include:

- **Basis for planning an audit.** Workpapers from a prior audit provide an auditor with background information for conducting a current review in the same overall area. They may contain descriptions of the entity, evaluations of internal control, time budgets, audit programs used, and other results of past audit work.
- **Record of audit work performed.** Workpapers describe the current audit work performed and also provide a reference to an established audit program. (See Chapter 13 on preparing audit programs.) Even if the audit is of a special nature,

such as a fraud investigation where there may not be a formal audit program, a record should be kept of the auditing work carried out. This workpaper record should include a description of activities reviewed, copies of representative documents, the extent of the audit coverage, and the results obtained.

- **Use during the audit.** In many instances, the workpapers play a direct role in carrying out the specific audit effort. For example, the workpapers can contain various control logs used by members of the audit team for such areas as the controls over responses received as part of an accounts receivable customer balance independent confirmation audit. Similarly, a flowchart might be prepared and then used to provide guidance for a further review of the actual activities in some process. Each of these elements would have been included in the workpapers in a previous audit step.
- **Description of situations of special interest.** As the audit work is carried out, situations may occur that have special significance in such areas as compliance with established policies and procedures, accuracy, efficiency, personnel performance, or potential cost savings.
- **Support for specifi audit conclusions.** The final product of most internal audits is a formal audit report, as discussed in Chapter 17, containing audit findings and recommendations. The documentation supporting the findings may be actual evidence, such as a copy of a purchase order lacking a required signature, or derived evidence, such as the output report from a computer-assisted procedure against a data file or notes from an interview. The workpapers should provide sufficient evidential matter to support the specific audit findings that would be included in an audit report.
- **Reference source.** Workpapers can answer additional questions raised by management or by external auditors. Such questions may be in connection with a particular audit report finding or its recommendation, or they may relate to other inquiries. For example, management may ask internal audit if a reported problem also exists at another location that is not part of the current audit. The workpapers from that review may provide the answer. Workpapers also provide basic background materials that may be applicable to future audits of the particular entity or activity.
- **Staff appraisal.** The performance of a staff member during an audit—including the auditor's ability to gather and organize data, evaluate it, and arrive at conclusions—is directly reflected in or demonstrated by the workpapers.
- **Audit coordination.** An internal auditor may exchange workpapers with external auditors, each relying on the other's work. In addition, government auditors, in their regulatory reviews of internal controls, may request to examine the internal auditor's workpapers.

In some respects, audit workpapers are no different from the formal files of correspondence, e-mails, and notes that are part of any well-managed enterprise. A manager would keep files of incoming and outgoing correspondence, notes based on telephone conversations, and the like. However, these files are based on good practices and may vary from one manager to another in an enterprise. The manager may never be called on to retrieve these personal files to support some enterprise decision or other action.

Internal audit workpapers are different in that they may also be used to support or defend the conclusions reached from the audit. They may be reviewed by others

for various reasons. Members of an internal audit enterprise may work on common projects and need to share workpapers to support their individual components of a larger audit project or to take over an audit performed previously by another member of the audit staff. It is essential that an internal audit department have a set of standards to ensure consistent workpaper preparation.

(a) Workpaper Standards

There is no specific form or format for internal audit workpapers. The Institute of Internal Auditors professional standards, outlined in Chapter 8 (see www.theiia.org), contain only high-level guidance for audit workpapers through its 2330 standard:

> *Internal auditors should record relevant information to support the conclusions and engagement results.*

This is a very broad standard, but it is supported by a series of Practice Advisories that provide additional supporting information on internal audit workpaper issues, including their preparation, control of the documentation, and retention requirements. The actual style and format of workpapers, however, will vary from one internal audit department to another and, to a lesser extent, from one audit to another. An internal audit department often establishes workpaper standards that are consistent with those of external auditors. However, internal audit should always recognize the differences between the financial statement attestation work of external auditors and the operational aspects of internal auditing. While there is no requirement to adopt external audit workpaper standards, many internal audit functions find it convenient to follow the general format of their external auditor's workpaper approaches.

Workpapers are not designed for general reading or as noninternal audit management reports. They are designed primarily to support individual internal audits and may be used by other members of the internal audit function, including management and quality assurance as well as external auditors and corporate legal functions. The workpapers should follow a consistent set of standards and be able to stand alone so that an authorized outside party, such as an external auditor, can read through them and understand the objectives of the internal audit, the work performed, and any outstanding issues or findings. Internal audit workpaper standards should cover the these areas:

- **Relevance to audit objectives.** The content of the workpaper must be relevant to both the total audit assignment and any specific objectives of the particular portion of the review. There is no need for materials that do not contribute to the objectives of the specific audit performed.
- **Condensation of detail.** An internal auditor typically gathers a considerable amount of detailed data and information on any review. That material should be carefully summarized in the audit workpapers to better describe the audit activities performed. For example, an audit may make use of CAATTs, as discussed in Chapter 21, to confirm balances on a data file, but often it is not necessary to include the entire CAATT-produced output in the workpapers. A totals summary with test results, some sample details, and a copy of the computer program used may be sufficient.

- **Clarity of presentation.** To present clear and understandable material, auditors and their supervisors should review workpaper presentations on an ongoing basis and make recommendations for improvements.
- **Workpaper accuracy.** Workpaper accuracy is essential for all audit schedules and other quantitative data. Workpapers may be used at any time in the future to answer questions and to substantiate later internal audit representations.
- **Action on open items.** Questions frequently are raised during an audit, as part of the internal auditor's workpaper notes, or information is disclosed that requires follow-up. On completion of the audit, there should be no open items in workpapers. All workpaper items should either be cleared or formally documented for future audit actions.
- **Standards of form.** For workpapers to accurately describe the audit work performed, they must be prepared in a consistent format within any audit workpaper or from one workpaper to another within the internal audit department. An internal audit manager should, for example, know where to find an auditor hours schedule for any workpaper reviewed. The standards of form should include:
  - **Preparation of headings.** Individual workpaper pages or formats should have a heading with the title of the total audit, the particular component of that total audit assignment contained in a given workpaper sheet, and the date. A smaller heading on one side should indicate the name or initials of the person who prepared the workpaper and the date of preparation.
  - **Enterprise.** The use of appropriate headings, spacing, and adequacy of margins facilitates reading and understanding. The auditor might think of this enterprise along the lines of the manner in which a textbook is organized.
  - **Neatness and legibility.** These qualities not only make the workpapers more useful to all readers, they also confirm the care that went into their preparation.
  - **Cross-indexing.** All workpapers should be indexed and cross-indexed. Cross-indexing provides a trail for the auditor and assures the accuracy of information in the workpapers as well as in the subsequent audit report.

(b) Workpaper Formats

As mentioned, workpapers were once lengthy paper documents, handwritten by auditors with samples of any reports and other exhibits included in the package. With the now-pervasive use of laptop computers to develop and document internal audit work, those older workpapers are far less common today. Exhibit 16.5 shows a manually prepared workpaper page from an operational audit of a physical inventory observation. Although the exhibit is in a text font that implies manual, handwritten preparation, the same page can be developed through word processing software. The important point here is this is a brief auditor description of an internal auditor's observations. This form can stand on its own. The reader can determine the entity it covers, who did the work and when, and how this workpaper sheet relates to others in the audit. This basic format is used in other exhibits in this chapter and throughout the book. Internal auditors must be particularly careful to document all work steps and all audit decisions. For example, if an audit program had a work step that the in-charge auditor determined was not appropriate for a given review, the auditor should explain why that step was deleted rather than just marking it "N/A." In some situations, the initials of the audit supervisor who approved the change should also

EXHIBIT 16.5 Manually Prepared Workpaper Sheet Example

	Global Computer Products Internal Audit	
AR-2.5.1	*Audit: MAXXAM Plant Inventory Observation*	*RRM*
	Location: South Bluff March 4, 20xx	*3/4/xx*

Internal audit observed the taking of a finished goods physical inventory at the MAXXAM div. plant in South Bluff, OH. We reviewed the physical inventory instructions issued by the plant controller's office (see X-Ref-01) and found them complete and satisfactory. Plant personnel started the inventory at 8:00 AM on March 3. Internal Audit observed that all other plant activities were shut down during the inventory taking and that counting proceeded in an orderly manner.

Worksheets for recording the counts were prepared using Global Computer's inventory system—they listed the parts assigned to designated storeroom locations but with no actual quantities (see X-Ref-02). A representative from the controller's office—Lester Tuttle—headed the control desk, issued count sheets, and logged them upon receipt.

As part of the inventory observation, internal audit selected a series of random stock-keeping numbers and independently took test counts. We compared these counts to the counts recorded by the inventory team. Test counts and results were summarized (see X-Ref-03).

As a result of this physical inventory observation, internal audit found . . .

be included. Similarly, if the auditor was following up on a matter from a prior audit, the workpapers should document the manner in which the problem was corrected or else who advised the auditor that it had been fixed. It is not sufficient just to mark it "corrected" with no further references.

Internal auditors should always remember that situations may change and workpapers may be called into question many years after they have been prepared. It is possible for a regulatory agency, such as the SEC, to obtain the rights to see a set of workpapers prepared years ago as part of an investigation. The agency might ask further questions or take other steps based on the audit work and observations recorded in those old workpapers. Memories often fade, and the audit workpapers may be the only credible record.

Today, most internal auditors prepare their workpapers on their laptop computers, where many of the auditor commentaries and schedules are maintained on secure files and folders. Alternatively, workpapers may be organized as $8\frac{1}{2} \times 11$-inch sheets secured in three-ring binders. Some workpapers may use the much older format of folders prepared on legal-size sheets bound at the top. Regardless of page size or media, the purpose of a workpaper sheet is to provide a standard framework for documenting internal audit activities. As discussed, workpaper pages should be titled, dated, initialed by the preparer, and prepared in a neat and orderly manner. The next sections expand on this basic workpaper format.

(c) Workpaper Document Organization

A typical internal audit includes gathering a large amount of materials to document some internal controls process or the results of audit testing. With the wide range of activities reviewed and the equally wide range of audit procedures, the form

and content of those individual workpapers may vary greatly. The major categories depend on the nature of the audit materials and the work performed, and the workpaper standards should be built around some specialized types of files. This chapter refers to these as *files*; the term *folders* also is common today. Some internal audit departments still use the older term *binders* to refer to different workpaper groupings. Just as in any manual filing system, workpaper materials are classified by their basic type and grouped together in a file or bound together in a binder in a manner that aids their retrieval. For most internal audits, workpapers can be separated into these broad audit areas:

- Permanent files
- Administrative files
- Audit procedures files

(i) **PERMANENT FILES** Many audits are performed on a periodic basis and follow repetitive procedures. Rather than capture all of the data necessary every time a periodic audit is performed, certain data can be gathered into what is called a permanent workpaper file, which contains data of a historical or continuing nature pertinent to current audits. Some of these data may include:

- Overall enterprise charts of the audit unit
- Charts of accounts (if a financial audit) and copies of major policies and procedures
- Copies of the last audit report, the audit program used, and any follow-up comments
- Financial statements about the entity as well as other potentially useful analytical data
- Information about the audit unit (descriptions of major products, production processes, and other newsworthy matters)
- Logistical information to help the next auditors, including notes regarding logistics and travel arrangements

A permanent file is not meant to be *permanent* in that there never will be changes; rather, it provides an internal auditor starting a new assignment a source of background material to help plan the new audit. The permanent file is a source of continuity to tie audits together over time. Auditors sometimes are guilty of loading up these audit files with materials that do not deserve permanent status (e.g., copies of various procedures that will have changed by the time of the next audit). Materials readily available at the time of the next audit need not be retained in permanent files unless certain ongoing procedures were based on those earlier materials. Similarly, auditors sometimes fill up paper-based permanent files for out-of-town locations with maps and menus of local restaurants. These references will change as will both individual auditor preferences and department policies. This administrative planning material should be kept to a minimum.

(ii) **ADMINISTRATIVE FILES** Although a separate workpaper administrative file may not be necessary for a smaller audit, the same general administrative workpaper materials should be incorporated in all audit workpaper sets. If there is only a single auditor or limited review, this material may be incorporated into the single workpaper.

EXHIBIT 16.6 Workpaper Audit Program Example

B25	Global Computer Products Internal Audit Audit: Headquarters Direct Sales AUDIT PROGRAM—CASH	LCT 10/31/xx
Ref.	Audit Procedure	Disposition
1.a	Review sources of reducing difficult-to-control cash conditions.	W/P B.32 LCT 10/30/xx
1.b	Determine that physical safeguards are adequate for providing cash at all stages of operations.	
1.c	Review procedures to keep cash on hand—in all forms and levels.	
2.a	Determine that petty cash and branch funds are utilized and operated on an impress basis.	
2.b	Assess adequacy of documentary support for petty and miscellaneous cash disbursements.	W/P B.37 LCT 10/29/xx
2.c	Review controls surrounding issuance and use of company credit cards.	
3.a	Determine all employees who handle or have direct access to cash are adequately bonded.	
4.a	Select one of the petty cash funds and independently observe a cash count, reconciling results to recorded records.	W/P B.26 LCT 11/05/xx

(iii) AUDIT PROCEDURES FILES Records should be maintained of the actual audit work performed, depending on the type and nature of the audit assignment. For example, a financial audit may contain detailed spreadsheet schedules with auditor commentary on tests performed. An operational audit may contain interview notes and commentary on auditor observations. This file is generally the largest for any audit and often contains these elements:

- **Listings of completed audit procedures.** Workpapers are a central repository documenting the audit procedures, and include copies of the audit programs along with the initials of the auditors and the dates of the audit steps. Commentary notes may be on the programs or attached as cross-referenced supplementary notes. Exhibit 16.6 shows a completed audit program filed in the workpapers.
- **Completed questionnaires.** Some internal audit functions use standard questionnaires covering particular types of internal control procedures. These questionnaires normally provide for yes and no answers and appropriate supplementary comments.
- **Descriptions of operational procedures.** Workpapers should briefly describe the nature and scope of a specific type of operational activity. This description can be a process flowchart, as discussed earlier in this chapter, or a verbal narrative. The auditor should always note on the workpaper the source of information to develop this description. A member of auditee management may have described the process, or the auditor may have gathered this information through observation.
- **Review activities.** Many internal audit workpapers cover specific investigations that appraise selected activities. These can include testing of data, observations

EXHIBIT 16.7 Travel Audit Workpaper Example

	Global Computer Products Internal Audit	
	Audit: Headquarters Travel & Entertainment	RRM
Z12.4	AUDIT PROGRAM—CASH	10/31/xx

Internal Audit reviewed a sample of employee travel and entertainment reports filed electronically during the 3rd quarter, 20xx. During that period, 987 reports were filed. We selected a sample of 45 reports for our review based on these criteria:

- All reports for the 6 senior officers — 16 reports reviewed.
- Reports involving international travel — 2 reports reviewed.
- All other reports having total reported expenses > $5,000 — 7 reports reviewed.
- A sample of the remaining 987 reports filed — 27 reports reviewed.

Our review was based on Global Computer Product's travel and entertainment procedures, dated 03/12/20xx. Selected sample reports were reviewed for these criteria:

- Reported expenses with policy guidelines.
- Use of the company credit card where appropriate.
- Use of company designated air carriers and rental cars.
- Appropriate levels of management approvals.

The results of the review are summarized on . . .

of performance, inquiries to designated individuals, and the like. This is perhaps the most common type of workpaper prepared by the internal auditor. It follows no one form but serves only to describe the audit activities performed and the results. Exhibit 16.7 shows a workpaper covering tests of an audit of travel and entertainment expenses.

- **Analyses and schedules pertaining to financia statements.** In a financial-oriented audit, a special variety of workpapers relates to attesting to the accuracy of financial statement or account balances. This type of workpaper schedule is an appropriate documentation for the Sarbanes-Oxley Section 404 reviews discussed in Chapter 4.
- **Enterprise documents.** There are often basic enterprise documents, such as enterprise charts, minutes of meetings, particular policy statements or procedures, contracts, and the like. While some of these might be more appropriate for the permanent file, others are unique to a particular audit. However, the auditor should not include all material in the workpapers. For example, it may be sufficient to include a table of contents and have relevant extracts rather than incorporating an entire procedures manual in the workpapers. The purpose of these documents is to help future auditors in their decisions or processes.
- **Findings, point sheets, supervisor notes, or drafts of reports.** Point sheets describing the nature of the audit finding as well as workpaper references to the detailed audit work should be included in audit procedures files even though a copy has been forwarded to the administrative file. During an audit, the in-charge auditor or audit supervisor prepares review comments that may require explanation by the auditor. In some cases, further audit work is needed. A workpaper point sheet is shown in Exhibit 16.8. For smaller audits that do not have an administrative file, draft versions of the written report should be included here. These drafts can be annotated to show major changes, the persons

EXHIBIT 16.8 Workpaper Supervisor Point Sheet Example

A.4.2	Global Computer Products Internal Audit Audit: Axylotl Plant Production Control Workpaper Review Notes	RRM 11/08/20xx
W/P Ref.	Supervisor Review Notes	Auditor Actions
B-21 & C-21	Missing W/p X-references.	Corrected
B-16	Schedule does not crossfoot to D-02 summary—please revise and correct.	OK – See D.02.1
D-20	Does the ref. point to larger control problem?	OK – See D.02.1
D-21	W/P sheet not signed or corrected.	Corrected
D-36	Evidence does not support your recommendation—clarify!	
D-41 to 5	Missing W/p X-references	Corrected
—	Where is the X-Cat software located?	See XCM folder.

responsible for authorizing those changes, and in some cases the reasons for the changes.

- **Audit bulk files** Internal audits often produce large amounts of evidential materials, which should be retained but not included in the primary workpapers. For example, internal audit may perform a survey that results in a large number of returned questionnaires. These materials should be classified as workpapers but should be retrieved from the bulk file only as necessary.

Workpapers are the basis for audit documentation from one audit or auditor to the next and are also a means of communication with the enterprise's external auditors. An internal audit department should establish some overall standards covering the style, format, and content of the workpapers used in various audits. Some specific details do not need to be frozen, given the various types of audits performed and evolving audit automation procedures. However, workpaper contents should be prepared consistently for all audits. The audit procedures workpaper file, for example, should contain materials covering each of the areas just listed.

(d) Workpaper Preparation Techniques

Much of the process of preparing workpapers involves drafting audit comments and developing schedules to describe the audit work and support its conclusions. This detailed process requires that internal auditors follow the overall audit department standards for the preparation of workpapers and also make the workpapers easy to follow and understand. An important aspect is to ensure that all members of the internal audit staff understand the purposes for and the criticality of their audit workpapers. These supporting workpaper schedules will be reviewed by internal audit management and others, who may question the type and extent of the work performed based on whatever is documented in the workpapers. This section discusses some of the basic techniques needed for preparing adequate workpapers. These comments are based largely on today's more common laptop-prepared

workpaper templates but also include more traditional, manually prepared workpapers. Whether prepared manually or using a computer-based system, audit workpapers should contain certain indexing and notation standards that will allow for easy review by other interested audit professionals.

(i) **WORKPAPER INDEXING AND CROSS-REFERENCING** Similar to reference notations in textbooks, sufficient cross-references and notations should allow an auditor or reviewer to take a significant reference and trace it back to its original citation or source. For example, a workpaper document describing a financial review of fixed assets might mention that the IT application that calculates depreciation has adequate controls. It is sufficient to provide a cross-reference so that the interested reader can easily find those depreciation computation controls auditor review workpapers. Index numbers on workpapers are the same as volume and page numbers in a published book. Workpaper index numbers should tie into a table of contents, which usually appears on the first page of the workpaper folder or manual binder. The number identifies the specific page in the specific workpaper binder. References to this number elsewhere allow an auditor to select immediately the correct workpaper binder and page. The system used for index numbers in a set of workpapers can be as simple or complex as desired. Many internal audit departments adopt the same general indexing system used by their external auditors so that all members of the audit staff can understand the correct reference to a volume in a given workpaper set. A method for indexing manually prepared internal audit workpapers might follow a set of three digits so that "AP-5-26" would mean the 26th page section of the 5th step in a given set of audit procedures. If multiple pages were required for page 26, they would be expressed as AP-5-26.01, -26.02, and so forth. Any numbering system should be easy to use and adaptable to change. With laptop-based workpaper documents, Microsoft Word hyperlinks can be a useful tool.

Cross-referencing refers to placing other reference workpaper index numbers within a given workpaper schedule. For example, a workpaper schedule may discuss controls over fixed-asset additions and state that all additions above some specified limit receive proper approval by management. That workpaper statement would parenthetically reference another workpaper index number denoting fixed-asset tests and indicating evidence of management approvals. Cross-reference numbers are particularly important in financial audits, where all numbers on various schedules should be tied together to assure consistency.

(ii) **TICK MARKS** Going back to the early days of manually prepared audit workpapers, auditors often prepared a financial or statistical schedule and then selected various numbers from that schedule on which to perform one or more additional tests. For example, an auditor may review a sample of purchase orders to determine if they represent vendors on the approved list, are subject to competitive bids, are computed correctly, and so forth. Rather than list this sample of purchase orders on multiple workpaper sheets for each of the tests, auditors normally prepare one schedule, using what are called *tick marks* to footnote various tests performed.

Tick marks are a form of auditor manual or pencil shorthand notation that has evolved over the years, particularly for financial audits. An auditor can develop a particular mark to indicate that a given value on the financial schedule cross-foots to other related values and another tick mark to indicate that it ties to the trial balance. The auditor need only note somewhere in the workpapers the tick mark

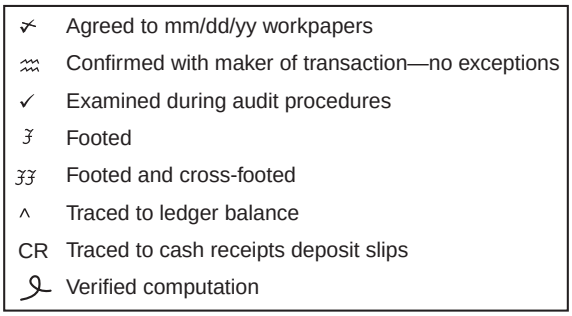


EXHIBIT 16.9 Workpaper Auditor Tick Marks Examples

used for each. Rather than asking the auditor to develop a legend, many internal audit departments have a standard set of tick mark symbols for use in all workpapers. For example, a check mark with a line through it means that the workpaper item was traced to a supporting schedule and the numbers at each were correct. These standard tick marks should be used by all members of the audit staff for all audits.

Standard tick marks improve communication, as audit management can easily review and understand workpapers. Exhibit 16.9 illustrates a set of traditional tick marks developed in the pencil-and-paper days. Although these same symbols may not be available through Microsoft Word, similar special characters can be designated for the same purpose. Of course, auditors might develop another mark to indicate some other type of cross-check performed in the course of an individual audit, which then must be clearly explained.

(iii) REFERENCES TO EXTERNAL AUDIT SOURCES Internal auditors often record information taken from outside sources. For example, an internal auditor may gain an understanding of an operational area through an interview with management. The auditor would record that interview through workpaper notes and rely on that information as the basis of further audit tests or conclusions. It is always important to record the source of such commentary directly in the workpapers. For example, a workpaper exhibit could show how the auditor gained an understanding of a sample system, and the source that provided that information should be documented.

Auditors may need to reference laws or regulations to support their audit work. Similarly, they may perform a vendor-related review and access a Web search to verify vendor existence. It is usually not necessary to include in the workpapers a copy of what may be a voluminous regulation, or a copy of a page from the search. However, workpapers should clearly indicate the title and source of all external references, including the Internet address if appropriate. Extract page copies can be included to make a specific point when necessary, but a reference notation is normally sufficient.

(iv) WORKPAPER ROUGH NOTES When conducting interviews, internal auditors often make very rough notes, written in a personal form of shorthand readable only by the author. Auditors should rewrite or reenter these rough notes into workpaper commentary. Because there may be a reason to review them again, these original note sheets should be included in the workpapers, placed in the back of the workpaper manual binder or even in a separate file.

Historically, most workpapers were prepared in pencil. Schedules were recorded on accounting spreadsheet forms, commentaries were written in longhand, and any exhibits were attached. Most internal audit departments have now automated their workpapers through the use of spreadsheet and word-processing software. This automation does not change the workpaper standards, but it usually makes the workpapers easier to read and to access. The typical workpaper today may use a mix of manual and automated schedules and audit commentaries. However, today's workpaper is usually a computer systems folder with perhaps some references to paper documents.

Technology is always changing, and we may be seeing different formats of audit evidence supporting audit workpapers in future years. Digital image scanners are very common today. They can be passed over a paper document, creating a digital image of that document for later audit evidence retrieval. Similarly, some computers are now equipped with a pen stylus for the user to "write" directly on the computer screen. The data are captured on computer files. These and other evolving technologies offer opportunities for audit workpaper automation.

(e) Workpaper Review Processes

All workpapers should go through an independent internal audit review process to assure that necessary work has been performed, that it is properly described, and that audit findings are adequately supported. The chief audit executive (CAE), reporting to the audit committee, has the overall responsibility for this review but usually delegates that work to supervisory members of the internal audit department. Depending on the size of the audit staff and the relative importance of a given audit, there may be multiple reviews of a set of workpapers, one by the in-charge auditor and another by a more senior member of internal audit management.

Evidence of this supervisory review should consist of the reviewer's initials and dates on each workpaper sheet reviewed. Some internal audit functions prepare a memorandum or workpaper review checklist to document the nature and extent of their reviews. In any case, there should be documented evidence that all workpapers have received a proper level of supervisory review. In addition to initialing completed workpapers, the supervisory reviewer should prepare a set of review notes with any questions raised during the review process to give to the responsible auditor for resolution. Some of these review points or questions may simply highlight clerical errors, such as missing cross-references. Others may be of a more significant nature and may require the auditor to do some additional follow-up work. Review questions should be cleared promptly, and the reviewer should take responsibility to ensure that any open questions are resolved. This workpaper review process should *always* take place prior to the issuance of the final audit report. This will ensure that all report findings have been properly supported by audit evidence as documented in the workpapers.

16.4 Internal Audit Document Records Management

Efforts to document processes or to describe an internal audit processes through effective workpapers are of little value unless an internal function has a strong document retention function covering all of its work products, including auditor

notes, copies of meeting minutes, IT files, and many others. As we move to largely paperless business and internal audit environments, this document retention need has become much more of a challenge than in the old days of paper-and-pencil records. In those old days, documents were often retained in formal filing cabinets. Access required getting a key from an office administrator, supervisor reviews were evidenced by a familiar signed initial on the form, and attempts to make unauthorized changes resulted in smudged erasures. The ease and flexibility of things today raises document risks, such as the loss of audit workpapers due to a stolen laptop to process errors in a CAATT developed by internal audit.

In the first section of this chapter, we discussed internal audit documentation requirements and outlined the need to keep all relevant internal audit documentation for seven years after the completion of an internal audit. This can sometimes cause a challenge in our paperless auditing environment today. Operating systems or file formats may change, and we may not be able to access or read a document. Documents can disappear due to someone mistakenly hitting DELETE, or documents can disappear because of a failure to download an auditor's laptop system to a central server system. An internal audit function needs to implement strong and consistent document management policies with assigned administrative responsibilities for the tasks.

Chapter 18 discusses IT general controls and IT Infrastructure Library (ITIL) best practices. Many of the latter ITIL best practices cover such areas as establishing configuration management controls over IT resources and IT change manage processes. While ITIL focuses on the IT infrastructure, many of best practice concepts apply to internal audit document management. The next list discuss some important or even essential needed document management practices for an internal audit function in today's environment of auditor laptops and wireless networks:

- **Document standards and review processes.** Internal audit needs to establish standards for the software used, laptop computer configurations, and general document and template standards. The goal should be that every member of the internal audit team is using the same equipment and—with the exception of some specialized IT tools—everyone is following the same formats and standards. An objective of an internal audit's documentation processes should be to eliminate all separate paper documents. When an internal auditor needs to use paper forms or other evidential materials, digital scanners should be employed to capture the material.

  Formal and secure processes should be set for each scheduled audit. An internal auditor at a field location may be assigned a laptop with a preliminary audit program as well as workpapers from a prior review all secured and loaded. The lead auditor may encounter situations where an established audit program needs to be modified, but these proposed changes can be passed through a secure virtual private network for review and approval by audit management. That audit work, loaded on the lead auditor's laptop and shared with others on the audit team, should be the prime records repository for a given internal audit. At the conclusion of the audit, the workpaper materials—including the audit report—should be downloaded to the audit department's central server system.
- **Backup, security, and continuity.** This is perhaps the most critical and high-risk area for laptop-based internal audit systems. Many of the cybersecurity and

privacy controls discussed in Chapter 20 are very appropriate for automated internal audit work as well. A good starting idea here is to configure and assign auditor laptop systems as internal audit tools only. There should be no outside links to the Internet or permitted downloads to USB devices. For personal e-mails back home and the like, an internal auditor can use one of the many small portable devices available.

While we should not chain an audit laptop to the internal auditor's body, strong security measures should be applied to keep the system secure. Strong security and password controls should be installed such that if a system is stolen, its contents cannot be easily accessed. (We use the word *easily* because strong computer forensics experts can access almost anything.) Procedures should also be established for internal audit files to be backed up and downloaded to the internal audit server system on a regular basis.

- **Hardware and software resource management.** Once some internal audit functions used central IT records for their automated workpapers. Today, with relatively efficient and lower-cost resources available, there is really no strong reason why an internal audit function does not have a server system dedicated to just internal audit purposes. A secure system should be installed as a repository for all internal audit activities. The system's key file folders should be folded in with the IT function's continuity planning processes, as discussed in Chapter 22.
- **CAATT repository.** Chapter 21 discusses IT tools to improve access and improve audit efficiencies. All too often, these tools and processes were viewed as part of the "IT audit" specialist's domains and kept separate from other internal audit documentation and materials. Every effort should be made to group and organize all CAATT-related materials with other internal audit workpaper records.
- **Audit reports, risk management, and internal audit administration.** Internal audit has a need to prepare and distribute a large body of materials, including audit reports, risk management analyses, budgets, and communications with the audit committee. The same seven-year document retention rule should apply to these internal audit administrative records, and they should be placed in secure folders on the audit department server system.

The seven-year retention rule can place demands on physical storage facilities. Many enterprises have used secure storage facilities for off-site storage of their older paper documents that have retention requirements. Vendors will pick up an enterprise's critical documents, catalog them by some broad retrieval categories, and then store the in secure, fire-protected facilities. These storage vendors provide insurance-company protection of stored documents and will deliver any document requested in a relatively short time frame. Although originally oriented to paper documents, similar vendors provide retention facilities for electronic documents. Internal audit should make arrangements for some type of secure off-site storage for key internal audit digital and paper documents.

16.5 Importance of Internal Audit Documentation

Adequate documentation is required for virtually all internal audit processes. This chapter has emphasized the importance of audit workpapers to document internal

audit activities as well as process modeling to describe enterprise activities. The ability to prepare descriptive and effective workpapers is a key internal CBOK requirement. In addition, all internal auditors, from the CAE to audit staff, should be comfortable and familiar with the many IT tools available to describe and document internal audit processes.

Note

1. Securities and Exchange Commission, *Retention of Records Relevant to Audits and Reviews,* www.sec.gov/rules/final/33-8180.htm.

CHAPTER 17

Reporting Internal Audit Results

An audit report is a formal document in which internal audit summarizes its work by reporting its observations and recommendations. Audit reports are the most important end product of the internal auditing process and are a major vehicle by which to describe internal audit's activities for people both inside and outside of the enterprise. Audit reports provide evidence about the professional character of internal audit activities and allow others to evaluate this contribution. Effective audit reports, of course, must be supported by high-quality audit fieldwork, as discussed in Chapter 9, but that same audit fieldwork can be nullified by poorly written or ill-prepared reports. The preparation of clear and effective reports should be a major concern for internal auditors at all levels, from the chief audit executive (CAE) to audit team staff members. The understanding of how to construct and draft an effective internal audit report is a basic common body of knowledge (CBOK) requirement.

Good internal audit reporting is more than just report preparation and appearance. Audit reports should reflect the basic philosophy of an enterprise's total internal audit approach, including its underlying review objectives, supporting strategies and major policies, procedures covering the audit work, and the professional performance of the audit staff. While the audit report is the major means of communication, internal auditors will be less effective if their communications with the rest of the enterprise are limited only to published reports. Communication also must be effected through interviews during the course of fieldwork, closing meetings when audit findings are first presented, meetings with senior management and the audit committee to apprise them of the results of audits, and many other contacts throughout the enterprise. All members of the internal audit enterprise must be effective communicators in both their written and spoken words. This chapter discusses the purpose and presentation styles of internal audit reports, including various formats and methods of presenting the results of audit work to management and others in the enterprise. Audit reports are a major component of internal audit communication.

17.1 Purposes and Types of Internal Audit Reports

Internal audit reports have a basic purpose to describe a planned and scheduled audit and to communicate the results of that audit. By their nature, internal audit reports are generally critical and tend to emphasize such matters as identified internal controls weaknesses. While it is perfectly proper to report that internal audit reviewed some area and found no problems, if the audit department or some individual consistently found no problems in most of its scheduled audits, there may be a need to review

internal audit's risk assessment approach or to reexamine its activities. Whether a formal written document circulated to senior and board-level management or an informal verbal presentation at the end of the audit fieldwork, all internal audit reports should always have four basic objectives and components:

1. **Objectives, timing, and scope of the review.** The audit report should summarize the high-level objectives of the review, where the review took place, and the high-level scope of the internal audit. The scope statement, for example, might disclose that the audit was performed at the request of the audit committee or was initiated as the result of a discovered fraud.
2. **Description of findings** Based on the conditions observed and found during the review, the audit report should describe the results of the audit. Often this section is where the report describes what, if anything, is wrong with the conditions found, as well as why it is wrong. The term *wrong* here includes internal control weaknesses, violations of company procedures, or any of a wide variety of other internal audit concerns.
3. **Suggestions for corrections.** Audit reports should include recommendations, based on the findings, for correcting the conditions and their causes. The objectives of these report suggestions include statements about fixing observed conditions as well as recommendations to improve operations.
4. **Documentation of plans and clarificatio of views of auditee.** The auditee may wish to state mitigating circumstances or provide a clarification of issues for any reported matters in disagreement. Depending on the report format, this section is often a place where the auditee can formally file a response to the internal audit findings and state plans for corrective actions in response to those audit findings and recommendations.

This four-step process of (1) why internal audit launched the review, (2) what internal audit found to be wrong and why is it wrong, (3) what should be done to correct matters, and (4) what will be done by the auditee forms the basis of virtually all internal audit reports. Internal auditors should always keep these four steps in mind when drafting audit reports and the separate audit findings that provide the basis for these audit reports.

While internal audit functions often spend considerable time in preparing audit reports, sometimes they lose sight of who is the report reader. An internal audit report should be prepared for the audit committee, the unit that was audited, and responsible senior management. While audit committees are much more visible and prominent today due to Sarbanes-Oxley (SOx) regulations, the audit report management readership exists at all levels, including the management of the component reviewed and more senior levels of management up to the audit committee at a highest level. Each management group has special needs and interests, and these audit reports should serve overall enterprise interests. More specifically, the question comes down to whether internal audit's responsibilities are to the direct auditee or to the management group with overall or higher level responsibility for the area being audited.

The auditee—that is, the staff and management group that was audited—will be motivated by a combination of enterprise and local entity interests. Direct auditee management knows that its ultimate welfare is closely related to total enterprise success but knows also that these rewards are largely determined by its own performance. This perception of performance is a combination of the operational results

achieved and how more senior management thinks the directly responsible managers are actually contributing. In everyday terms, local or unit management strives to look good to upper-level management. What this all means in terms of internal audit is that the local managers often want help, but want it on a basis that does not discredit them with more senior levels of management. Ideally, they might like to have internal audit work with them on a private consultant basis but not report finding any dirty linen to senior management. While the internal audit professional standards discussed in Chapters 8 and 28 recognize that internal auditors sometimes may act as internal consultants, that is not internal audit's prime role.

Internal audit should try to help local management do a more effective job, knowing that in order to identify internal control problems and recommend potential solutions, it must have the full cooperation and a near-partnership relationship with them. However, this cooperative attitude can place pressure on internal audit if it is asked to pull its punches in audit reports that are copied to the audit committee and senior management. Internal audit may feel that its reported concerns will be implemented sooner if it does not criticize local management too harshly in its published audit reports. However, internal audit has a major responsibility to report within the audit's objectives on the conditions found or observed. While providing service to local management, internal audit's obligations reach all the way up to the audit committee of the board.

As a starting point for resolving these potentially conflicting demands, all management levels must have a comprehensive understanding of each other's needs and internal audit's responsibility to serve them. There is often a need for audit report recipients to increase the level of tolerance and flexibility by raising the level of findings and issues considered sufficiently significant to warrant inclusion in an audit report. This way, internal audit can eliminate many of the more minor matters that should be, and can be, finalized at the local level without involving higher-level managers. A determined joint effort is needed between the local managers and internal audit to work out necessary follow-up actions during the course of an internal audit.

The general effect of these actions is to push internal audit more toward being seen as providing a service to local management in its work and away from being viewed as a headquarters spy. This approach must continue to recognize that internal audit always has its important reporting responsibility to senior management and the audit committee.

17.2 Published Audit Reports

Although audit reports have been discussed as almost a single concept, they can take a variety of different formats and styles, ranging from Web-based documents to hardcopy paper reports. In any format, an audit report is a formal report document outlining internal audit's concerns and recommendations following the four objectives discussed previously. In past years, management sometimes placed restrictions or constraints on internal audit that limited it from preparing effective audit reports. For example, some senior managers, in the past and the days of paper documents, may have declared that all audit reports must be one page or less in size. This type of request sometimes occurred because internal audit functions wrote up pages and pages of audit report findings that may have seemed significant to the internal auditor but not to senior management.

The significance of audit reporting has changed after SOx. In the congressional hearings leading to the act, criticism was directed at audit committees that sometimes received only summarized reports but did not receive any level of detail regarding the audit findings. With SOx, audit committee members, and, of course, senior management are to receive full copies of all audit reports. While it is their right to request summarized reports as well, they are still responsible for receiving and understanding all reported audit findings. Internal control findings must be clearly described in an internal audit report. This section discusses formal published audit reports as well as alternative mechanisms for internal audit reporting.

(a) Approaches to Published Audit Reports

The form and content of internal audit reports can vary widely. An audit report covering a review of internal controls may appear different from a report on business continuity controls or one on fraud investigation procedures. However, no matter the subject of the internal audit, formal audit reports should always cover a similar general format, starting with a cover page, a description of the work performed, and then the internal audit findings and recommendations. We are describing an audit report in the sense of an older, multipage type of document. Today, a report is typically in a Web-based document that may never be formally printed. However, just as the words in a printed book cannot be changed once printed, software-copy versions of audit reports should be protected in a manner that no one but the author—internal audit—can change them after release or publication.

Just as a traditional book begins with a cover page and preface, an audit report should begin with an introductory page. Exhibit 17.1 is an example of an audit report introductory page for a formal audit report covering a review of the purchasing function in our Global Computer Products sample enterprise. This report's introductory page or pages should have these elements:

- **Title of report and objectives of review.** A brief, definitive title tells the reader what is contained in the audit report and is also useful for various summary reports. Similarly, an audit report should have a brief but clear statement of the review objectives.
- **Report addressees and carbon recipients.** An audit report should always be addressed to the one senior-level person responsible for addressing report findings, often someone usually at least one organizational level above the auditee. There should also be a selected list of carbon-copy recipients, as determined by internal audit. Copy recipients include the auditee's manager, members of senior management, and other interested persons, such as the partner in charge of the external audit team. (As an aside, we are using an archaic term here—carbon copy—even though carbon copy paper has all but disappeared in much of the world today. Of course, we mean additional copies.)
- **Audit scope and date of the fieldwork** Usually included with the statement of audit objectives is some abbreviated information on the general scope of the audit and the approximate date of the audit fieldwork. A statement that a given report covers a review of the "purchasing function for electronic components at the XYZ division" leads the reader to expect a different report from a statement that the audit covered just the "purchasing function."

EXHIBIT 17.1 Internal Audit Report Introductory Page

Inter Audit Department Audit Report
Peerless Division Purchasing Function

Global Computer Products

To: Malcolm Muddle, Director of Operations
CC: Amos Arrons, Peerless Division Finance
Cecelia Clark, Peerless Vendor Management
Sam Sneed, Debits & Credits, CPAs

The Global Computer Products internal audit department has performed an internal controls review of the Peerless Division purchasing function. The objective of our review was to assess the quality of the internal control environment and the control procedures operating over the Peerless headquarters facility at Burning Stump, NE. Our work was restricted to operations at the Burning Stump facility and did not include purchasing activities at the facility in Malaysia. We completed the fieldwork for this audit on XX, 20XX.

Our review included an assessment of the adequacy of Peerless Division purchasing processes in place and their compliance with overall Global Computer Products procedures. We performed detailed tests of procedures, as we felt appropriate, and also reviewed controls over key Peerless Division IT systems. In addition, we performed a detailed confirmation and quality assurance assessment of a sample of Peerless vendors.

We generally found the internal control controls over the Peerless purchasing function to be adequate. We did find some areas where we feel corrective actions are necessary to improve the internal control structures. Our internal audit findings and management's planned corrective actions are included in this report.

Samantha Smith
Internal Audit, Nov 7, 20XX

- **Locations visited and timing of audit.** Because of potential delays in wrapping up audit reports, time may pass between the date of the fieldwork and the final published audit report. The report cover page should clearly state when the audit fieldwork was performed and also mention the locations visited.
- **Audit procedures performed.** A brief paragraph describing the audit procedures performed is often very helpful to the report reader. This information is particularly useful if internal audit has performed some special testing procedures in order to arrive at its opinion. In this area, internal audit might mention its use of statistical sampling, for example, as discussed in Chapter 9.
- **Auditor's opinion based on the results of the review.** An internal audit report should *always* have some fairly general assessment of the overall adequacy of the controls or other concerns in the area reviewed. For example, the opinion statement might be worded using one of these examples:
  - "We found the controls in the area reviewed to be adequate except for . . ."
  - "We found that most controls were good and were operating as installed . . ."
  - "We identified significant control problems in the areas reviewed. Our findings . . ."

  The statement of the auditor's opinion can take many forms. However, it generally points to the detailed audit findings and recommendations, which follow these first pages of the full audit report. Exhibit 17.2 contains some

EXHIBIT 17.2 Informal Memo Format Audit Report Example

MEMO

To: Sam Sneed, Purchasing Dept.
From: Samantha Smith, Internal Audit
Date: Thursday, October 10, 20XX
Subject: Audit of Purchasing, Interim Report

ExampleCo Internal Audit has completed its review of the Heavy Iron Division purchasing function. Our fieldwork was started on September 5 and included visits to the Heavy Iron offices and additional testing as we found necessary. We have concluded our fieldwork for this review as of October 5, and this memo represents an interim audit report covering said fieldwork. A formal audit report, requiring your plans for corrective actions, will be released after we complete certain additional audit work, including purchase order confirmations.

We generally found internal controls over Heavy Iron purchasing function operations to be adequate. However, we also found certain internal control weaknesses requiring additional Heavy Iron Division investigation and correction actions. Although these comments may be subject to revision when we complete all of our audit work in this area, we have initially identified these control weaknesses.

- Despite frequent, multiple use of certain parts, blanket purchase orders allowing for price/volume discounts are not used.
- There appears to be little effort to seek bids from multiple vendors for some common commodities. Multiple vendors might yield lower prices.
- Security over purchasing files is weak. Although the function is largely automated, many product lines still use substantial paper records. There is no effort to protect those records during nonbusiness hours.
- The automated purchasing system needs an upgrade or overhaul. The system now in use is over 15 years old, has poor documentation, and cannot interface with several other key systems.

These comments are very preliminary and will be discussed in greater detail, along with our recommendations for corrective action, in our draft audit report to be issued after the completion of our final audit work. If there are any questions during the interim, please contact me.

examples of other auditor findings, including an opinion statement. No one form is right. The audit department's style should be consistent with senior management's wishes.

Internal audit reports often follow one of several common approaches. Given the type of enterprise, its overall management style, the skills of the internal audit staff, and many other factors, each of the audit report formats described has its own merits as well as disadvantages. Internal audit wants to communicate what it did, what it found, and what needs to be corrected in a manner that will gain the attention of key managers in the enterprise. All professionals are faced with a barrage of paper documents as well as electronic communications, which they are asked to read, understand, and act on. Internal audit wants to provide the readers of its reports with enough information to explain the issues but not so much that members of management will place the report aside with little more than good intentions of reading it later. Without enough information, the reader may not know if a serious problem or other issues requiring action exist. In an overly detailed report, the reader may miss significant points given the large volume of the materials

presented. Alternative approaches to developing and issuing internal audit reports include:

- **Audit reports with "encyclopedic" coverage.** Some internal audit reports strive to present a great deal of information about the activity area reviewed. Their objective is to provide an in-depth reference source to the report reader. The information can be of a historical nature or pertain to the current situation. It may cover operational practices and results or may deal with financial information. An example here might be a review of a complex finance-oriented automated system or a description of a complex manufacturing process.
- **Description of the audit procedures performed.** Audit reports sometimes provide a great deal of—sometimes too much—information about the audit procedures actually performed. Audit steps may be described in some detail, as might the scope of actual verification and testing. Sometimes this audit report coverage almost repeats the materials contained in audit standards and procedural manuals, as discussed in Chapters 7 and 8. With this type of audit report, there may be a question as to how interested the reader is in these procedural details and what purpose they really serve. Most users of audit reports should be willing to rely on the competence of internal audit for those technical dimensions. Detailed descriptions are of value only when internal audit needs to describe a complex area, such as the decision logic forming an opinion based on audit statistical sampling parameters. On balance, such detailed accounts of technical procedures should be excluded or at least minimized.
- **Detailed explanations of audit findings** Some internal audit reports go into voluminous detail about the results of the various audit efforts. Although the coverage here may look impressive, it is often doubtful whether an extensive amount of detail describing the audit findings serves a useful purpose. With a very large audit report "book," the reader may be turned off and thus miss the important materials. Web-based audit reports can summarize the findings and reference background information through hyperlinks. An internal audit report should not bury the reader with more information than most need. Audit reports should give only a necessary and sufficient amount of information about audit findings and allow the reader to understand the detailed issues involved.
- **A highly summarized report.** In the other extreme, some internal audit departments release very summarized reports that say only that internal audit has reviewed some topic area and usually found no control exceptions of significance. This same style of report often mentions that control exceptions were found and they were corrected, with no detail. These reports often do little more than state that internal audit has reviewed an area and found some "minor items," which were not included in the report even though they might be of interest to a reader. Unless these summarized reports reference longer, more detailed explanatory materials, they are not effective for most internal audit reporting needs. In addition, the summarized report may put the audit committee reader at risk by glossing over potentially significant internal control weaknesses and by not providing the details required under today's SOx rules.
- **Focus on significan issues.** The more common report format—often the best—is one that focuses only on "significant issues" that have potentially important bearings on internal controls weaknesses, policies, operational approaches,

the utilization of resources, employee performance, and the results achieved or achievable. More senior enterprise managers are interested primarily in problems that are of such a nature and scope. They typically wish to be informed and given the opportunity to contribute to solutions. If these significant issues relate to completed actions, the issues would have to be still more significant to merit the reporting. The advantage of this focus on significant issues is that senior managers can get the information they need without wading through excessive detail.

The actual audit report format and method of presentation varies from one enterprise to another. Exhibit 17.2 shows an example of positive-sounding audit report. Although this is a memo-format report and only one page in length, multiple-page reports should follow the same general style. While audit reports were once hardcopy typed documents, desktop- or laptop-based word-processing software has changed the style and format of audit reports today. Audit reports can now be issued with interesting typeface fonts, with supporting graphics, or in a totally electronic format over a proprietary intranet. However, no matter what the basic format, an audit report should always contain the elements of what internal audit did, when it did the work, and what it found. A key portion of an internal audit report should be the auditor's findings and recommendations.

(b) Elements of an Audit Report Finding

During a review, the internal auditors assigned to the project may encounter exceptions or internal control weaknesses in some of the areas to review, as outlined in the established audit program. (See Chapter 13 on how to prepare an audit program.) Those identified exceptions as well as other internal audit observations are the subject of the audit report findings. For example, the audit program may direct the auditor to review a sample of travel expense vouchers to check that they are properly approved and to verify that the reported expenses are consistent with published travel policies. If internal audit finds that some of the samples selected are not properly approved or are not in compliance with travel policy, internal audit will have one or more potential audit findings to report.

Auditors will encounter a large number and variety of these exceptions in the course of almost any review. Some may be relatively important—such as the discovery that significant numbers of vouchers submitted for payment lack proper approval signatures. Others may be relatively minor—such as the discovery of an employee who reported $25.50 for meal expenses when policy requires that such expenses must be less than $25.00. While the latter is a violation of policy, senior management may not be too interested in an audit report that is filled with these relatively minor infractions. This is not to say that an internal auditor should look the other way at such minor internal control items. Such smaller internal control exceptions should be documented and discussed with management at the conclusion of fieldwork. However, they may not necessarily be the type of issues to report to the audit committee and senior management through a formal audit report unless a series of them represent a trend. Then internal audit might consider the items through a summarized finding covering the overall condition.

An internal auditor must analyze the bits and pieces of information gathered during a review to select findings and recommendations for inclusion in the final

report. At the conclusion of the audit fieldwork, internal audit should always ask itself whether there was sufficient information to develop an audit finding, and, if so, how these matters of audit concern should be presented. Options for the latter range from informal discussions with local management to a formal presentation in the audit report.

Audit report findings presented in a common format allow the report reader to understand the audit issues easily. No matter what the nature of the audit work or the finding, readers should be able to scan an audit finding and quickly decide what is wrong and what needs to be corrected. While audit report findings are important both to internal auditors who drafted a finding and to report readers, sometimes the findings are not well constructed. Poorly drafted audit findings often make report readers question what the problem is and why they should be concerned. Good audit report findings should contain:

- **Statement of condition.** The first sentence in a report finding should summarize the results of internal audit's review of the area of concern. It can give a comparison of what is with what should be. The what-is sentence summarizes the condition or appraisal made by internal audit based on the facts disclosed in the review. The purpose is to capture the report reader's attention. Examples of audit report finding statements of condition include:
  - "Obsolete production equipment is being sold at bargain rates and in a manner that does not follow fixed-asset disposition policies."
  - "The backup and continuity plan for the new customer billing system has not been tested and does not follow enterprise security standards."
  - "The ABC division work-in-process inventory is not correctly valued according to generally accepted accounting principles."
- **What was found?** The finding should discuss both the procedures and the results of those procedures. Depending on its complexity, the finding can be summarized in little more than one sentence or may require an extensive discussion describing the audit procedures. This what-was-found statement can be as simple as "Based on a sample of employee expense reports filed for fourth quarter 20XX, the enterprise's preferred rental car agency was not used in over 65% of the expense reports reviewed." Often this portion of the finding is much more extensive, as internal audit describes the procedures performed and what was found. Examples can be found in the Exhibit 17.3 sample audit report findings.
- **Internal audit's criteria for presenting the finding** Audit findings should always have a criterion, or a statement of what should be used in judging the statement of condition. Without strong criteria, there cannot be an audit finding. Criteria vary according to the area audited and the audit objectives. The criteria may be the policies, procedures, and standards of an enterprise. In some instances, internal audit must develop the criteria. In an audit of the effectiveness of some procedure, there may not be preestablished targets or measurements that can be used as indicators, and standards may be couched in general or vague terms. Internal audit should consider these issues:
  - **Criteria of extremes.** Clearly inadequate or outstanding performance is relatively easy to appraise. However, when performance moves closer to the average, it becomes more difficult to judge. Internal audit sometimes can use extreme cases of inadequate performance as criteria for the report finding.

EXHIBIT 17.3 Audit Report Findings Sample

I. *Blank Purchase Orders*

Blanket purchase orders would allow the organization to receive supplies of frequently used common parts without the need to issue a separate purchase order for each commodity replenishment. Company purchase department policies allow and even encourage the use of these blanket orders, at buyer discretion. We found that several buyers of small commodity parts have never used the blanket purchase order concept. They generally advised us they thought they could get better prices by negotiating each purchase separately.

We reviewed the pattern of purchase orders for several frequently purchased commodities and found opportunities for potential savings. For example, separate purchase order arrangements with different vendors were made for certain electronic switch units. Vendor prices varied up or down by about 5% over the nine months reviewed. A blanket purchase order might have provided a guaranteed price, based on total aggregate quantities purchased.

Recommendation. A program of blanket purchase orders should be initiated for frequently used commodity-type parts. Price versus total quantity agreements should be negotiated with key supplying vendors. The purchasing department should monitor the cost savings and other benefits from the program.

II. *Professional Travel Expenses*

The company travel policy specifies that all employees should work with the company travel agent to find the lowest airfares for business travel. In addition, policy specifies that traveling employees should always attempt to be at their business destinations by 12:00 noon on the first business day of their trips. We found that this travel policy is largely ignored by employees in certain company departments. For example, almost all air travel arrangements for employees of department 22-88 were made individually by employees, ignoring the travel agent. Expenses were charged to corporate charge cards with no evidence of efforts to seek minimal air travel cost. Similarly, in our review of travel records over the past six months, we found over 5% of employees ignored the lowest-cost recommendation of the agent and selected higher-cost air tickets. Frequently, these same employees made air travel arrangements that brought them to their destination late on the first day of the trip.

Recommendation. Policies should be strengthened to encourage least-cost air travel. A revised policy statement should be developed and issued to all travel-mode employees, emphasizing the need for lowest-cost travel. When employees do not accept the travel agent's least-cost recommendation, the fact should be printed on the air ticket travel itinerary included with the employee's expense report. Departmental managers should be assigned first-tier responsibility to reduce their employee's air ticket travel expenses.

III. *After-Hours Office Security*

Company policy specifies that all office employees should clear their desks of all reports, memos, and other business papers at the end of the business day and also should sign off from their desktop computers. In a review of office areas on three successive evenings during the period of our fieldwork, we found numerous desks covered with work materials and numerous computer systems still left running. These practices compromise company security due to the possibility of unauthorized persons viewing materials left in desk areas.

Recommendation. All employees should be reminded of after-hours desktop policies. The security department should visit office areas from time to time in the evening. Persons not in compliance with after-hours policy should be reminded with a desktop security department note.

Although usually too extreme or incendiary, this might cause internal audit to state that some observed condition was "almost as bad as. . . ."

- **Criteria of comparables.** Comparisons can be made between similar operations or activities, determining their success or lack of success and causes for the differences. While it is never good to state specifically that Department A is X% worse than Department B, the report might compare the conditions found to average or typical conditions throughout the enterprise.
- **Criteria of the elements.** In some cases, internal auditors incorrectly state their performance criteria with such broad terms that it is impossible to evaluate the reported condition. This type of vague criteria states "All managers should make good decisions," for example. While ideal, we all know exceptions exist regularly. The reported measure should be broken down on a functional, organizational basis or by elements of cost related to specific activities.
- **Criteria of expertise.** In some cases, internal audit may find it useful to rely on other experts to evaluate an activity. These experts may be outside the enterprise or may be part of the audited enterprise's staff. This type of supporting reference often strengthens the overall audit finding.

- **Effect of the reported finding** Internal audit should always consider the question: How important? when deciding whether to include an item in the audit report. Internal audit must weigh materiality—if the finding is of no significance, it may not be a finding at all. Once a decision has been made to include it as a finding in the audit report, the effect of the reported condition should be communicated. Findings that will result in monetary savings or that affect enterprise operations and achievement of goals are always of special interest to management.
- **Cause or reason for the audit deviation.** The answer to the question: Why? is especially important to management when reading an audit report. The reasons for a deviation from requirements, standards, or policy should be explained briefly but as well as possible. Identifying a cause for the condition provides management with a basis for taking needed action.
- **Internal audit's recommendation.** Audit report findings should conclude by recommending appropriate corrective actions. This is the audit finding's conclusion: What should be done? A recommendation can be a simple admonition to fix something or can be a fairly detailed set of suggested corrective actions.

Although internal audit's description of objectives, audit procedures performed, and the opinion of the controls as a result of the review are all important elements in an internal audit report, members of management will evaluate the quality of the report on the basis of the reported findings and recommendations. If any facts reported in an audit finding are incorrect, no matter how close to the real truth they are, auditees often challenge the credibility of the overall audit report. Any misstatement can place the entire audit report into question. Internal audit should *take extreme care* to report its audit findings factually and accurately. Otherwise, a significant amount of good internal audit work can be ignored. Care should also be taken in developing strong, meaningful, and realistic recommendations. The recommendations generally should consider the costs and benefits of various alternative recommended actions. Of course, if the audit finding is highlighting a potential violation of the law, the recommendation should always be to take prompt and complete corrective action.

(c) Balanced Audit Report Presentation Guidelines

If an internal audit's objective is to evaluate the efficiency, economy, and effectiveness by which management has accomplished its objectives, then internal audit has a responsibility to disclose both the satisfactory and the unsatisfactory conditions found during an audit. While conditions needing improvement should always be described, communications here should minimize the description of audit findings in totally negative terms. Rather, internal audit should strive to encourage management to take needed corrective action and to produce results. An internal audit report cannot be fully successful if the auditee is not receptive to the results of the audit, but a report with findings that just talks about what was right also provides little help to management. Consequently, internal audit should adopt a positive reporting style that is balanced with a mixture of favorable as well as appropriate unfavorable comments, that always presents matters in perspective, and that emphasizes constructive rather than just negative comments.

To provide a level of balance, internal audit must sort through the various positive and negative data gathered during the course of a review and ask itself: What should be the type and extent of favorable comments to be reported as a result of this audit? The answer cannot be laid down in precise terms. The same criteria used in identifying significant findings can be used to report items considered significant based on standards of performance. For example, assume that an audit objective was to evaluate the timeliness of completing purchase requisitions. Comments in a report finding should relate to the enterprise's ability or inability to complete these purchase requisitions in a timely manner and ignore other unrelated issues. Some techniques to provide better audit report balance are:

- **Provide audit reports with perspective.** Internal audit should avoid the temptation to cite only those factors that support its conclusions and to ignore those that distract from them. Perspective is always added when listing the monetary effect of a finding as well as the value of the entire account under review. A $1,000 error sounds much more severe when it is part of a $100,000 account than it does for a $10 million account. The report finding should disclose, as appropriate, the total monetary amount audited or recorded in relationship to the total value of errors encountered. This procedure makes evident the significance of the finding. Also, when deficiencies are disclosed in only part of the area examined, balance will be added to the report by identifying those areas examined that did not contain deficiencies. This practice should be in accordance with an internal audit policy of disclosing accomplishments as well as deficiencies.
- **Report auditee accomplishments.** Since the evaluation process involves weighing both satisfactory and unsatisfactory aspects of auditee operations in light of the audit objectives, mentioning auditee accomplishments in improving controls or correcting errors together with the noted deficiencies or aspects in need of improvement can increase the usefulness of the audit report as a management tool. The auditee accomplishments should be disclosed in the report summary when the audit conclusions audit may be affected by their significance and in the findings when a detailed disclosure of the accomplishments is desired or necessary.
- **Show planned actions.** In situations where the auditee has taken, or has made plans to take, corrective action prior to the completion of the audit, the audit

report should disclose this fact. In addition, other steps taken by the auditee in an attempt to correct a reported deficiency may not be so obvious but nevertheless should be considered as a positive reportable action. For example, the auditee may have contracted with an outside consultant to help implement the internal controls needed in an information technology application covered in an audit report. Such arrangements should be included in the report along with those control weaknesses.

- **Report mitigating circumstances.** Mitigating circumstances generally consist of factors relating to the problems or conditions discussed in the audit report over which management has little or no control. Since these factors lessen management responsibility for the condition, they should be reported as part of cause. Mitigating circumstances, for example, may include the very short time frame in which a program was required to be implemented, business conditions requiring immediate changes, or a lack of adequate budget funds for adding personnel or other resources to accomplish objectives.
- **Include the audit responses as part of the audit report.** Auditee responses to a finding may contain information that provides additional balance to an audit report. In addition to planned corrective action, the auditee may indicate other related accomplishments or cite additional facts and other circumstances. In instances where agreement has not been reached on the finding or recommendation, the auditee should be given the opportunity to explain the basis for nonoccurrence.
- **Improving audit report tonal quality.** The use of positive and constructive words and ideas rather than negative and condemning language will give the report a positive tone. Unless they are deserved, audit reports should avoid phrases indicating that the auditee "failed to accomplish," "did not perform," or "was not adequate," and should state audit report ideas in a positive and constructive manner. Audit reports with negative audit findings titles and captions should be avoided since they do not add to the finding and may even misrepresent the actual situation. Thus, a negative-sounding title for a finding such as "Inadequate Controls over Company Cash Controls" might be replaced by "Cash Controls Need Improvements" or just "Cash Collection Procedures" followed by a discussion of the internal audit concern.

These comments are not meant to suggest that all audit reports should be sugarcoated and that internal audit should never make strong critical statements about auditees. An internal audit and its subsequent audit report often can be a very critical process, where internal audit investigates an area that perhaps has not received much management attention. If internal audit finds serious problems in the area reviewed, it should clearly identify problems that might be significant unless prompt corrective actions are taken. When possible, however, internal audit should give credit where due and discuss either positive or mitigating circumstances as would be appropriate. Exhibit 17.4 contains some examples of negative and positive audit report findings.

(d) Alternative Audit Report Formats

With today's technology, audit results can be reported in a wide spectrum of formats. While the standard text-based audit report format described here is certainly familiar

EXHIBIT 17.4 Audit Report Negative and Positive Statement Examples

Negative Audit Findings	Positive Audit Findings
1a. We found that controls in the area were generally poor.	1b. We identified areas where controls need improvements.
2a. Little management attention has been given to keeping documentation current.	2b. The documentation was not current and other priorities have prevented it from being updated.
3a. The failure to reconcile these accounts was caused by a lack of management attention.	3b. We observed that these accounts had not been reconciled for several past periods.
4a. Documentation was either out of date or nonexistent.	4b. We found only minimal current documentation in this area.
5a. The new inventory system is poorly designed.	5b. The inventory system has some major control weaknesses. More attention should have been given to its design.
6a. This failure to protect passwords could result in a management fraud.	6b. Poor password controls are a weak internal control.
7a. No attention has been given to protecting stockroom inventories.	7b. Better controls should be established over stockroom inventories.
8a. The responsible manager did not seem to understand company procedures in this area.	8b. Training in the use of these procedures needs to be strengthened.
9a. The department failed in several of its training program operations.	9b. Several opportunities exist for strengthening controls in training program operations.
10a. The budgetary system was not adequate to assist management in the control of project funds.	10b. The establishment of a proper budgetary system would assist management in the control of project funds.

and often the best way to present audit work, internal audit can use other approaches to describe the results of its audit findings and recommendations. That standard report becomes a record of corporate governance activity allowing an enterprise to certify what internal audit did, what it found, and what was recommended. In our litigation-prone society, it is essential that an enterprise and its audit committee have formal, secure records of its internal audit activities. However, internal audit may elect to consider some alternative approaches, particularly for interim audit results reporting. Some of the less formal and more abbreviated alternative means by which internal audit can report the results of its work include:

- **Oral reports.** In a few situations, internal audit may want to report the results of its work and any recommendations orally. This reporting mode should always occur, at least on an interim basis, when the on-site audit team reports the results of its work at an end of audit fieldwork closing conference. In other cases, an oral report may be the result of emergency action needs, and an oral presentation may also be a prelude to a more formal written report. To some extent, there may always be oral reporting as a means of supplementing or explaining written reports, especially when individuals being served have special needs. Oral reporting is often useful, but it should be a supplementary form of audit reporting only.

An oral report should not be a substitute for the formal written report, as there generally is no permanent record beyond any meeting notes. The auditor may think that local management agrees to correct some problem, but management may not really say that. As a result, there are more likely to be misunderstandings later on unless detailed, contemporaneous notes are taken for workpaper documentation or if the meeting is taped. However, the appearance of a tape recorder or video unit usually causes distrust. Oral audit reports should be used carefully and not in lieu of later written reports.

- **Interim or informal memo reports.** In situations where it is deemed advisable to inform management of significant developments during the course of the audit, or at least prior to the release of the regular report, internal audit may want to prepare some kind of interim written report. These reports may pertain to especially significant problems where there is a need for prompt corrective action, or the reports may be a type of progress report. A memo report should be used, at a minimum to describe the results of an oral presentation, as discussed previously. An interim or memo report is often released to record the results of an oral presentation and to call local management's attention to a potential audit finding. The material discussed in this example report will eventually be included in a more formal audit report discussing the total results of an internal audit.
- **Questionnaire-type audit reports.** Usually some kind of written report is prepared at the completion of an individual audit assignment. A questionnaire type of report can be a useful interim summary to the formal audit report or serve as an appendix to the formal report document. This format works best where the scope of the audit review deals with fairly specific procedural matters, and usually at a fairly low operational level. This type of report usually has a fairly limited range of overall usefulness. Exhibit 17.5 is an example of a questionnaire audit report. It is perhaps best used as an educational tool to inform management of internal audit's concerns.

EXHIBIT 17.5 Questionnaire-Format Audit Report Example

ExampleCo Heavy Iron Division Audit of Purchasing, October 29, 20XX Summary of Internal Control Strengths and Weaknesses	Result
1. Are departmental operating procedures current and adequate?	**YES**
2. Are purchasing requirements properly specified by requesting departments?	**YES**
3. Are multiple bids sought for all regular, noncustom purchases? *Multiple bid procedures are regularly ignored.*	**NO**
4. Do requesting groups regularly send specifications with purchase requests?	**YES**
5. Are blanket purchase orders used for volume use parts? *Although procedures exist, blanket purchase order procedures are often ignored.*	**NO**
6. Have dollar-based authorization limits been set for all P/Os and are they followed?	**YES**

Note: The above is only a sample of what would be a much larger "yes" and "no" type of audit questionnaire report. Additional sheets could be attached to better explain "no" control weakness responses.

- **Regular descriptive audit reports.** In most audit assignments, the work should be concluded with the preparation of a formal descriptive audit report. The exact form and certainly the content of such written reports will vary widely, both between individual audit assignments and between individual internal audit departments. Reports may be short or long and presented in many different formats, including various approaches for quantitative or financial data presentations. The whole idea is that audit reports represent a documented record of internal audit's work on an assignment.
- **Summary and significan finding audit reports.** Internal audit functions frequently issue an annual (or more frequent) report summarizing the various individual reports issued, any significant findings, and the range of their content. These summary reports are often prepared for the audit committee or other members of senior management. Exhibit 23.5 shows an example of this type of significant findings report as part of a discussion on serving and communicating with the audit committee. Summary reports are especially useful to top-level managers, but they must be only cover pages for the senior managers and board members who have a SOx responsibility to have access to the full reports. In a larger internal audit enterprise, summary reports also allow the CAE to see the total reporting effort with more perspective, and on an integrated basis.

17.3 Internal Audit Reporting Cycle

Starting in the early work steps of an internal audit, it is often desirable to develop a framework for the final report, filling in as much as possible as the audit moves along. Information and statistics on the area to be audited can be gathered during the survey stage and included in the workpapers, as discussed in Chapter 16. Doing this will ensure that needed information is obtained early in the audit, and it will prevent delays in the final report-writing process. In addition, the objectives and scope of the review, defined at the start of the audit, should be fine-tuned as the audit progresses.

As audit findings are developed and completed, they can be inserted in the proper sections of the report, together with any preliminary comments by the auditee. The completed audit report is then just one step—although a very important one—in internal audit's overall process of evaluating and commenting on the adequacy of internal controls in order to serve management needs. The audit report process starts with the identification of findings, the preparation of a draft report to discuss those findings and related recommendations, a discussion of the audit issues identified with management along with the presentation of the draft report, the completion of management responses to audit report findings, and the publication of the formal audit report covering the area under review. Exhibit 17.6 outlines suggested critical phases and action steps for the preparation of an audit report. Although a given internal audit department may alter some of these steps slightly to modify the report for its own needs, these steps generally are the process necessary to issue an appropriate internal audit report.

As findings are developed, the on-site internal audit team should review them with members of auditee management, soliciting their perspectives on the evolving audit findings. Possible causes for audit findings should also be discussed and additional information gathered to prove or disprove the potential audit report condition.

EXHIBIT 17.6 Audit Report Preparation Steps

1. Outline Audit Findings
    1. Determine if there is sufficient support to warrant the audit findings.
    2. Review to determine where additional evidence may be needed.
    3. Ascertain that all audit finding causes and effects of findings are considered.
    4. Determine whether there is a pattern of deficiencies requiring procedural changes or whether the findings appear to be isolated cases.
2. Prepare the First Draft Audit Report
    1. Review findings drafts for adequate development.
    2. Ascertain whether the findings are stated in specific rather than in general terms.
    3. Assure that all figures and other facts have been checked and cross-referenced in the workpapers.
    4. Review workpapers supporting all findings for adequacy of support and disclosure of items of significance.
    5. Check for adequacy of tone, punctuation, and spelling. (Note: Do not rely just on Word spell-checks!)
    6. Ascertain whether there is sufficient support for the expression of the auditor's opinion or whether a qualification is needed.
    7. Determine whether the cause, effect, and recommendations are adequately developed.
    8. Discuss methods of improving content and writing style with internal audit team.
    9. Prepare draft report clearly marked "DRAFT."
3. Discuss with Management
    1. Determine whether management was aware of the problem and already was taking corrective action.
    2. Find out management's reasons for the conditions.
    3. Ascertain whether there are facts or mitigating circumstances of which the auditor was unaware.
    4. Determine management's ideas on how to correct the conditions.
    5. Ensure that management is aware of all significant items that will be present in the report.
    6. Ensure that efforts are made to obtain management agreement on the facts and conditions.
4. Preparation of Final Audit Report Draft
    1. Ascertain that all prior recommendations for changes in report have been made.
    2. Ensure that management's viewpoints have been adequately considered.
    3. Determine that the report is well written and easily understood.
    4. Ascertain that summaries are consistent with the body of the report.
    5. Ensure that recommendations are based on conditions and causes stated in the findings.
    6. See that management's viewpoints are fairly stated and adequately rebutted, if necessary.
    7. Review report for use of graphics, tables, and schedules to clarify conditions presented.
    8. Ensure that auditors who wrote the findings agree with any changes made.
5. Audit Report Closing Conference
    1. Ensure that management has had an opportunity to study the final report.
    2. Attempt to obtain agreement on any points of difference.
    3. Consider any suggestions for changing content of report as well as specific wording.
    4. Obtain current plans for follow-up action from management.
6. Issue Final Report
    1. Ensure that final changes are made in accordance with the closing conference.
    2. Check report once again for grammar and typographical errors.
    3. Review report for a balanced presentation, with positive comments included on results of audit when applicable.
    4. Make final reading of report for content, clarity, consistency, and compliance with professional standards.

In some instances, enterprise personnel will assist in obtaining information to develop the findings. These personnel often will provide useful feedback as to whether internal audit's facts are correct and whether it is on the right track. Areas of disagreement can be pinpointed and resolved. Discussing findings with enterprise personnel at a staff level helps to get agreement and encourages implementing actions. When an agreement is reached, internal audit may be able to limit the amount of detail included in the audit report finding, thus shortening the audit report.

(a) Draft Audit Reports

Once the audit fieldwork has been completed and internal audit has discussed its proposed audit findings with the auditee, a draft audit report generally should be prepared. We have used the term *generally* since sometimes a draft report is not necessary if a special, investigative report is to be made for presentation to management. For example, internal audit typically would not prepare a fraud investigation draft report to review with persons involved in the potential fraud. In most other cases, internal audit should prepare a report draft with its proposed findings and recommendations along with a space for management responses. The draft is then sent to the manager directly responsible for the area that was audited. This is the person who responds and outlines the corrective actions to be taken. Internal audit then combines these auditee responses with the original report header pages and the draft findings and recommendations to produce the final audit report, as is shown in the Exhibit 17.7 example. This final draft report typically is presented as a last opportunity for the auditee to read and understand the tone and contents of the audit report to be issued.

Closing meetings and a draft report are important steps to validate the adequacy and accuracy of the reported findings and the soundness of the related recommendations prior to the release of the final audit report. While the major foundation for this validation is the audit work performed by the internal audit staff, such work needs to be supplemented by the review and confirmation of the auditee personnel. The benefits of this supplementary validation are twofold. First, it provides a cross-check on the accuracy, completeness, and quality of the audit work. Important facts may have been overlooked or erroneously interpreted. There may also be other factors affecting some particular matter that are known only to certain people. The exposure to the auditee thus provides an important check on whether the findings and recommendation will stand up under later scrutiny. The second benefit is to help promote a partnership relationship with local management that will create both a cooperative spirit and a commitment to working out adequate solutions.

This type of validation should go on during all stages of a review. One of the most important ways this is effected is through the presentation of the draft report to auditee management. Depending on the nature of the audit objectives and the complexity of the audit findings, the draft report can be presented at the closing conference at the end of the fieldwork, just preceding the departure of the field audit personnel, or delivered to the auditee after the completion of the fieldwork. Strategies for the timing of the draft report delivery include:

- **At the exit conference.** Internal audit generally finds it difficult to deliver a full draft audit report at the end-of-fieldwork exit conference. Many audits are just too complex, and there may be too many final questions or clarifications,

EXHIBIT 17.7 Final Audit Report Example

April 20, 20X2 Report No. X2-36

Mr. Bruce R. Weston, General Manager
Bright Products Division
The Wonder Corporation

Dear Mr. Weston:

The corporate audit department has completed an operational review of the internal control structure for the Bright Products Division engineering organization. Bright Products engineering has a FY 20X2 budget of $13,000,000 and is responsible for technical research, product design, and development of the Whatzit product line. As of March 30, 20X2, engineering had 1,018 employees, of which 916 were direct. The objective of our review was to evaluate the controls over equipment resource planning and utilization, compliance with policy, and the effectiveness and efficiency of the current plan of organization. Our audit included, but was not limited to, reviews of:

- General organization controls over engineering projects
- Controls over company utilization of capital equipment
- Controls over the accuracy of the reporting of indirect labor charges
- Departmental expenses, including a review of travel expense reports

This review covered operations during the period January 1 to December 31, 20X1. The review was made by Roger G. Wilson and his assistant, Connie Rodriguez, during the period February 13 to March 31, 20X2.

Our review found that the Bright Products engineering department is well managed, with generally good controls over its resources. However, we found that controls over capital equipment inventory should be strengthened. Our audit findings and Bright Products Division's plans for corrective actions are summarized below.

The internal auditing department wishes to express its appreciation for the very fine cooperation received during the review by the divisional management and personnel.

Respectfully submitted,
Charles W. Reiber, general auditor

The Wonder Corporation
Findings and Recommendations

Capital Equipment Inventory

Capital equipment is not under proper administrative control within the Bright Products engineering organization. The Equipment Capitalization Report, maintained by property accounting, is not used by the engineering organization on a regular basis. Although engineering has responsibility for the assets assigned to them, they have not taken a capital equipment inventory of that equipment for over one year.

We selected 50 units from the most current Equipment Capitalization Report and found the following:

- Three units with an original capitalized value of $119,402 could not be located during our fieldwork. One of these was found after the release of our draft report.
- Nine units were found to have no capital equipment serial number identification tags.

The cause for these expectations is the lack of sufficient capital equipment inventory verification procedures and the failure to consistently use serial number identification tag procedures.

(*Continued*)

EXHIBIT 17.7 Final Audit Report Example (*Continued*)

Recommendations
Engineering should utilize the existing property accounting reports to better control its capital equipment. All section managers installing engineering capital equipment should be reminded of the need to properly install identification tags on all newly installed equipment. In addition, engineering should take a full wall-to-wall inventory of its capital equipment and schedule period limited inventory reviews on an ongoing basis.

Management Responses
Copies of the Equipment Capitalization Report will be circulated to responsible managers on a regular basis. Procedures have been issued to remind engineering managers of the need to review that report and to assure that identification tags are properly installed.

A full inventory of installed capital equipment will be taken in June 20X2. Procedures will be developed to regularly cycle-count installed capital equipment.

or editing needed to allow draft audit reports to be delivered at the time of the exit conference. Providing the draft report at the exit conference typically works only for compliance-type audits of smaller field or branch locations where the recommendations are to correct less significant problems, such as mispriced goods at a local retail branch.

- **Before departure of the fiel audit team.** Here the audit team has discussed its concerns with local management in a formal exit conference and then prepares the draft report, including any additional comments or clarifications that may result from that conference. In most situations, this approach is more realistic than presenting the draft report at the time of the exit conference. However, the pressure to wrap up the audit work and get home may cause the audit team to take shortcuts in their desire to complete the field engagement. Again, this strategy works best with relatively simple audit assignments.
- **After the completion of fieldwork** With this strategy, the audit team has its exit conference but returns to the home office to draft the audit report over the next few days or even weeks. Many internal audit enterprises find this approach works best. Audit management has an opportunity to review the field team's work and to make adjustments, as appropriate, to the draft audit report. The risk here is that the internal audit team responsible for the review will be pulled in other directions and will not complete the draft audit report in a timely fashion.

Audit exit or closing conferences should include members of the audit team and the local management responsible for the area reviewed. At the conference, major findings and proposed recommendations are reviewed, and, to the extent that an agreement has already been reached between audit and local enterprise on particular matters, an opportunity is provided to inform responsible management in the area reviewed and to secure further agreement on audit findings and recommendations. The closing conference provides internal audit with a major opportunity to confirm the soundness of the audit results and to make any necessary modifications to the audit report draft as justified. This is also a major opportunity to demonstrate the constructive and professional services internal audit can provide. These meetings, although sometimes contentious, can be a major means for building sound partnership

relations with the auditee. The objective should be to get as much agreement as possible so that the audit report can indicate the completed actions.

In many situations, the draft report is forwarded to the local management for their review and corrective action comments prior to the finalization of the formal or final report. Local management and the actual auditees typically are given a limited amount of time to review this draft report, to suggest changes to its overall tone or to specific findings, and to prepare their audit responses. While internal audit should encourage auditee management to request changes to the draft report, the emphasis should be on the substantive issues in the draft report rather than on its wording.

Internal audit should request formal responses within perhaps 14 days after the receipt of the draft report. Although this is a relatively short time, given the time that the audit team has spent on its fieldwork and draft report preparation, auditee management should be able to develop a response rather rapidly since it is aware of the findings and suggested recommendations from the exit conference. However, both internal audit and auditee management should try to operate in the same general time frame. That is, if internal audit spends an inordinate amount of time preparing its draft report, auditee management should be given an even greater amount of time to prepare its audit report responses.

The submission of draft reports to auditee management at a later stage has merit through internal audit's demonstration of genuine consideration for the auditee. However, internal audit should work with auditee management to avoid excessive delay in finalizing the report. A major part of the effectiveness of the report is the extent to which it is issued promptly.

(b) Audit Reports: Follow-Up and Summary

Once management has submitted its audit report responses, internal audit should combine these responses with its draft findings and recommendations to release the final audit report. This report is addressed to management at least one level above auditee management, with copies to the board audit committee and other appropriate officers of the enterprise. A representative example of such a brief but complete final audit report is shown in Exhibit 17.7.

Once the final audit report has been issued, internal audit should schedule a follow-up review to ensure that needed actions based on the audit were actually taken. In some cases, management may request this procedure. While the desirability of follow-up action in itself is very clear, questions can be raised whether this is the proper responsibility of internal audit, and whether such action by internal audit will undermine the basic responsibilities of the managers in charge of the particular activities. Although internal audit standards, as discussed in Chapter 8, call for follow-up reviews, they can put internal audit more in the role of a police officer and could conflict with its ongoing partnership relationship with the auditee.

Internal audit should play only a limited, specific role after the audit report has been released, such as making itself available to respond to questions, and to review again the situation at the time of the next scheduled audit in the area. Many enterprises have adopted an intermediate type of approach where the coordination for audit report recommendation follow-up is placed in the hands of another office—usually within the controller's function or some more neutral administrative services group. The corrective actions are then initiated by the responsible line or staff manager, but responses are made to the coordinating group. If there are undue

delays in dealing with the recommendation, the coordinating office can issue a follow-up status report. Under this approach, copies of these responses can also be supplied to internal audit for information, or internal audit can maintain a liaison with the coordinating group. There is no single best answer as to how this follow-up effort should be handled, but on balance, it seems best to subordinate internal audit's formal role in it. Internal audit's help can always be requested on a special basis, either by the coordinating office or by individual managers. In addition, any lack of action can be highlighted at the time of the next scheduled internal audit review.

Internal audit has a responsibility to produce audit reports that are readable, understandable, and persuasive. The objective is to issue reports that will command the attention of the managers who have the responsibilities for the various operational activities and to induce them to take appropriate corrective action. A secondary objective is for audit reports that will build respect for the internal auditing effort.

Internal audit receives a final payoff in its knowledge of the actions taken by auditees based on the internal audit report recommendations. A combination of internal audit technical skills and the ability to communicate results to people in a way that will best ensure their acceptance and active support are elements of good audit reporting. The importance of this part of internal audit's work underlines the need to give audit reports careful attention. It means that the CAE should be actively involved in the audit report process, and all levels of the internal audit staff should think in terms of ultimate report needs. In this connection, the problems of report development should also be given proper attention in internal audit training programs. When reports are subsequently circulated, referred to, and implemented, they become a statement of internal audit's credentials. Audit reports are usually the major factor by which the reputation of an internal audit department is established.

(c) Audit Report and Workpaper Retention

Formal internal audit reports and their supporting workpapers are important documents supporting internal audit's activities. Procedures should be implemented to retain the records for each audit performed as part of regular enterprise-wide records storage procedures. While storage of these records was once treated more informally as a best efforts internal audit function decision, SOx rules have changed things. A major event associated with the fall of Enron and the impetus for SOx was the destruction of audit records by the company's external auditor. Because of this Enron external audit document destruction, SOx rules require that all audit-related records *must be maintained* for a period of seven years. While these rules were aimed at external auditors, they apply to internal audit as well.

All paper-based audit reports and supporting workpapers should be deposited in a secure corporate records storage facility. Some enterprises have their own procedures for this storage, but many others use outside providers, which place these documents in secure areas for later retrieval as required. While these external sources provide references to aid any later retrieval, internal audit should establish its own internal procedures to cross-reference audit work with the storage titles of the stored items.

We often think of stored internal audit records as paper binders of workpaper files, but today much internal audit work is developed on computer-based digital records, ranging from auditor notes entered on the auditor's laptop to photos of a

factory condition captured on the auditor's cell-phone camera. This material should be secure and then downloaded to a secure storage media. Material on laptop audit computers should be burned on to CD or DVD disks or other more permanent storage devices. For internal audit materials located on corporate servers or legacy systems, internal audit should make arrangements with the information systems enterprise to download and store internal audit records following the same procedures used for other centralized systems.

Internal audit reports and supporting workpapers can be supporting materials in litigation or even government legal actions. An enterprise may be required to produce records of its internal audit work to prove, in a court of law, what it did or did not do in some area. Also, a court order may require that the enterprise disclose records supporting some matter. The SOx seven-year record's retention rule says that an enterprise must take care to preserve and organize all supporting records covering many areas. Internal audit reports and supporting workpapers are important enterprise records that are subject to those same record retention rules.

17.4 Effective Internal Audit Communications Opportunities

Communications are an important element of every phase of internal audit's activities. Internal auditors communicate through formal audit reports, face-to-face encounters during audit fieldwork or meetings, and through a wide range of other formal and informal communications. When there is a misunderstanding or conflict on an audit assignment or when the auditor's recommendations are not correctly understood, an analysis of the difficulty usually points to some type of communication problem. Internal auditors should always keep in mind that communications are a basic ingredient of almost every type of audit activity and should work to improve these communications and reduce organization-level conflicts.

Effective communication both on a person-to-person basis and with larger groups is a key component to internal audit success. An internal auditor should have a good understanding of the problems associated with effective communications and how to cope with them. Situations continuously arise in an internal audit function when individuals need to communicate with each other. These include giving an oral instruction to a staff auditor, discussing an operational problem during an audit exit meeting, counseling a subordinate, interviewing a prospective employee, or conducting a staff performance review. All of these situations involve differing personal relationships but consist of a continuing two-way flow of messages. An internal auditor should understand this process in order to identify the kinds of problems that can distort or actually prevent effective communications. These problems affect all steps in the communications process and include:

- **Not giving proper consideration to the power relationships of message senders and receivers.** Communication with a line supervisor often is different from that with a senior officer.
- **Ignoring temporary emotional stress by either the sender or receiver.** An audit exit meeting often turns into a situation filled with conflict and stress unless the internal audit communicator takes care to consider these potential emotional issues.

- **Failing to properly evaluate the capacity of the recipient to receive and understand the message.** If internal audit encounters a severe control problem in a technical area in the course of its work, those issues must be communicated properly.
- **Use of words that can have multiple meanings or can convey unintended meanings.** We have discussed this concern when preparing audit reports, but this is all the more critical in verbal communications.
- **Undue haste in the transmission of messages that undermine clarity and/or credibility.** Messages often need to be communicated slowly so all parties will understand.
- **Perception that the sender wishes to satisfy personal needs, thus inducing emotional resistance and blocks.** Often others view internal auditors as people having a personal agenda. Others quickly recognize this, and communication may become blocked.
- **Failure to build needed foundations for the core message and related bad timing.** Internal audit concerns are not effectively communicated when they are just thrown in the lap of the auditee.
- **Lack of clarity or conviction because of a reluctance to cause the receiver dissatisfaction.** While an internal auditor must build a case to describe a concern convincingly, the auditor should never mince words to avoid describing a problem situation but should always clearly communicate a control concern.
- **Impact of nonverbal actions, such as tone of voice, facial expressions, and manner of communication.** For example, in some parts of the world, a crossed leg with the sole of the foot pointing to the listener can be viewed as an extreme insult.
- **Not giving consideration to the perceptions and related feelings of the recipient.** Auditors should try to understand how messages will be received and decoded by their receivers.

All of these problems are part of the larger need for internal auditors to put themselves in the receiver's perspective and to consider how their message will be received. When that internal audit message is communicated with some empathy, the result should be effective two-way conversation. The communicator must do everything practicable to understand how the receiver thinks and feels and then to communicate in a manner that gives all possible consideration to that knowledge. While the communicator often has conflicting higher-priority needs that prevent fully satisfying the receiver, it is still important to have a good understanding of the total communication process in order to make choices that are most consistent with the enterprise's overall welfare.

Both parties in communications—especially the main activator—learn from the questions and comments made by the receiver in response to a series of messages. This is called *feedback.* Part of effective two-way communication is to induce feedback so that an internal auditor has the best possible basis for determining whether managerial objectives are achieved. Different approaches may be necessary to induce and utilize this good feedback. A related component—listening—is important in order to utilize any feedback better and to demonstrate interest in the other person's views. Otherwise, the result of such a message can be to create an emotional response that significantly blocks the receiver's acceptance and understanding of the sender's intended message.

The varying needs of people relate alternatively to competition, conflict, and cooperation. Traditionally, conflict has been viewed as destructive and undesirable. However, when properly administered, conflict can be useful in achieving organizational welfare. Internal auditors need to learn to utilize conflict to the point where it is constructive but to control it when it threatens to get out of hand. Internal audit's responsibilities unavoidably generate situations that create competition and potential conflict. Both enterprise units and individuals continuously compete in terms of job performance, recognition, management support, and other needs. That competition should induce imaginative and sound thinking and high-level work performance. At the same time, the forces generated can be so intensive that the competitors seek any means to win, irrespective of the questionable propriety and legitimacy of those means. At that point, competition ceases to benefit the enterprise, and appropriate corrective actions are needed. Management then has a challenge to exploit the benefits of competition and healthy conflict in a legitimate professional sense but to control the process to avoid excesses. Internal audit becomes very much part of this set of competition and conflict concerns. In the course of their reviews, auditors often find themselves in conflict with various elements of an enterprise. Auditors can cause auditees to lose a level of competitive standing within their enterprises, and auditees may disagree with internal audit on just that basis. In the course of a review, conflict often occurs, and the effective auditor should use this conflict to communicate with management and convince it to take appropriate actions. However, the effective internal auditor needs to understand how to control that conflict.

Although the goal to win is an important and desirable motivation, it is the responsibility of every manager to make subordinates understand that sometimes there are other things more important than a particular victory. Put in other terms, people need to understand that how one wins is more important than the fact of winning. These principles also need to be reinforced continuously by the rejection of approaches that are not in the common interest. Internal audit must be continuously alert and watch for red flags that indicate potential problems. When problem situations are observed, decisive actions may be necessary. Rules may be amended, particular individuals disciplined, personnel assignments readjusted. Ideally, conflict should not be allowed to develop to the point where these more dramatic direct actions are necessary. The challenge is to utilize conflict but not to let it get out of control to such an extent that it is counterproductive.

In the typical enterprise, there is a continuing need to properly balance stability and change. Management seeks stability by developing policies and procedures whereby operations are standardized to improve internal controls and to ensure the best handling of recurring similar types of events. However, changing conditions call for amended policies and procedures. Finding a proper balance between stability and needed change is difficult because the factors involved are usually hard to analyze and measure. One obstacle to change is that enterprises often become used to existing policies and procedures and tend to become biased in their favor, thus making them unaware of and unresponsive to need for change. Internal audit often encounters this obstacle when it recommends policy or procedural changes through its audit reports. Additionally, people typically do not like to accept change even when the need for it is reasonably clear. Somehow, convenience tends to triumph over objectivity. For this reason, internal auditors often face a great deal of resistance when they suggest changes, irrespective of their real merits.

At the highest level, the need for change may involve new strategies, new business ventures, changes in products, or new supporting policies. Related changes may involve new organizational structures, relocation of plants, new production processes, or changes in people, but internal auditors often do not make recommendations for change at that level. In some cases, these changes involve only established habits or convenience, while others require more substantial adjustments. There is often some built-in resistance to change, ranging from minor attitudes to deliberate defensive action—including, in its most extreme form, sabotage. When a decision involving change has been properly made, any resistance, whatever it may be, should be minimized, eliminated, or at least reasonably controlled by management.

When making their recommendations, internal auditors should understand how the enterprise will deal with the change. How can internal audit achieve needed changes in a manner that will best serve higher-level enterprise welfare? In all cases, the nature and scope of the necessary actions depend on the significance of the particular recommended change. Because individuals place a high priority on their freedom of action, human considerations are especially important in the design and implementation of these controls. Since all managers are responsible for internal controls and at the same time are subject to them, the impact of recommended control improvements on people should be considered carefully. Perhaps in no phase of the management process is an understanding and consideration of people so critical.

17.5 Audit Reports and Understanding the People in Internal Auditing

This discussion on creating effective internal audit reports has focused on the interests of all internal auditors in connection with their relations with their audit committee, senior management, and to each other. While all of this is of interest to internal auditors as a part of their review and analysis of internal controls, it should also be of interest to the CAE and the audit committee. Some unique and specific problems confront internal auditors in their activities, including an image problem, because an auditor is often thought of as focusing excessively on detailed compliance or control issues and is viewed by many as threatening. As has been discussed in earlier chapters, this image may have been earned because of the manner in which internal auditors were once used in enterprises. To some extent, the image has also resulted because some internal auditors today do not do enough through their audit work and mode of personal relations to build a better image.

Today's internal auditor faces some serious problems in changing this image. Internal auditors are charged with certain protective responsibilities that tend to make others in the enterprise see them as antagonists or police officers. Internal audit's total role should go far beyond the narrow role of providing protective service. The modern internal auditor today is no longer the police officer or the person with the green eyeshade who is buried in what are sometimes viewed as trivial details. Instead, internal auditors should be concerned with total enterprise welfare at all levels and in relation to its activities. In all aspects, communications and relations with people are continuing challenges that involve a target for internal audit that is always moving forward. Internal audit's success in meeting that challenge provides

one of the greatest available opportunities to serve the enterprise and to achieve its maximum welfare.

We have stressed the internal auditor CBOK theme throughout this book. The ability to describe internal audit work and to make effective internal audit recommendations is a key internal audit CBOK requirement. However, going beyond the task of preparing and delivering effective internal audit recommendations and reports, all internal auditors should strive to be excellent communicators to and with the fellow internal audit teams and all members of their overall enterprise.

PART V

Impact of Information Technology on Internal Auditing

CHAPTER 18

IT General Controls and ITIL Best Practices

In today's world of information technology (IT) processes and computer systems, ranging from applications to control an enterprise's accounting general ledger to the all-pervasive Internet, internal auditors must have a strong understanding of IT internal control techniques. Although the lines of separation are sometimes difficult to understand, we generally can think of IT controls on two broad levels: application controls that cover a specific process, such as an accounts payable application to pay invoices from purchases, and what are called general IT controls. This latter category covers internal controls that are important for all aspects of an enterprise's IT operations; they cover more than just specific IT applications and include an enterprise's pervasive IT controls.

The concept of IT general controls goes back to the 1960s and the early days of centralized, mainframe computers. In those days, internal auditors sometimes looked for such things as an access control lock on a computer center door as a general control that covered all processes and applications operating within the centralized IT operations center. Today, we often think of the processes that covers all enterprise IT operations as the IT infrastructure. Because of the many possible variations in IT techniques today, there is really no one set of rights and wrongs that covers all IT general controls. An enterprise should implement a set of best practices that will serve as guidance for establishing its IT general controls best practices.

This chapter looks at IT general controls from an internal audit perspective and with an emphasis on IT general controls based on the worldwide recognized set of best practices called the information technology infrastructure library (ITIL). These ITIL recommended best practices outline the type of framework internal audit should consider when reviewing IT internal control risks and recommending effective IT general controls improvements.

Having a general knowledge of IT general controls should be an essential common body of knowledge (CBOK) requirement for all internal auditors. Many internal auditors believe that because they specialize in financial or operational audits, they do not need to understand general control issues. In fact, all internal auditors should have a CBOK level of understanding of IT general controls as well as the other IT issues discussed in chapters in this part of the volume.

18.1 Importance of IT General Controls

Internal auditors became involved with early IT audit and control procedures—then called data-processing controls—when accounting applications were first installed on early punched-card-input computer systems. Those early systems were often installed in glass-walled rooms within corporate lobbies to impress visitors with the enterprise's "sophistication." However, those same early systems were not particularly sophisticated. Internal auditors, who were then unfamiliar with data-processing technology, would "audit around the computer." That is, internal auditors might look at input controls procedures and the application's outputs to check whether the inputs balanced to the output reports. In this era, there was little question about the accuracy and controls of reports produced by a computer systems. Internal auditors would just focus on the inputs and outputs while going around the actual computer program processing procedures.

Things changed in the early 1970s with an extremely fast-growing California-based insurance company, Equity Funding. Some people believed the company was growing too fast. The company's external auditors decided to try a new technique and run their own audit software programs against Equity Funding's files. The result was the discovery of a massive fraud with invalid data recorded on IT application files. Under management direction, fictitious insurance policy data had been entered on computer files. Equity Funding's external auditors had previously audited around the computer system, relying on printed computer system output reports, with no supporting procedures to verify the correctness of computer programs and files. In the aftermath of the Equity Funding affair, the American Institute of Certified Public Accountants (AICPA) and the Institute of Internal Auditors (IIA) began to emphasize the importance of audits of data-processing operations and application controls. A new professional specialty, called *computer auditing,* was launched.

In those early days of business data processing, most computer systems were considered to be "large," and standard sets of auditor control objectives and procedures were developed for reviewing controls. Many of these objectives are still applicable today, but internal auditors must look at these IT control objectives from a somewhat different perspective when reviewing controls in a modern IT environment. The profession began to think of IT controls within specific applications and general controls surrounding all IT operations. IT general controls cover all information systems operations and include:

- **Reliability of information systems processing.** Good controls need to be in place over all IT systems operations. Discussed throughout this chapter, these controls often depend on the nature and management of the specific size and type of systems used.
- **Integrity of data.** Processes should be in place to ensure a level of integrity over all data used in various application programs. This control objective is a combination of the general operations controls discussed in this chapter as well as specific application controls discussed in Chapter 19.
- **Integrity of programs.** New or revised programs should be developed in a well-controlled manner to provide accurate processing results. These integrity control issues include the overall process of application program development and are part of our discussion in sections on ITIL best practices.

- **Controls of the proper development and implementation of systems.** Controls should be in place to ensure the orderly development of new and revised information systems. These control issues are discussed in Chapter 19.
- **Continuity of processing.** Controls should be in place to back up key systems and to recover operations in the event of an unexpected outage—what was called disaster recovery planning and is often known today as business continuity planning. These control issues are discussed in Chapter 22.

This chapter discusses general controls over in-house information systems operations ranging from client server systems to desktop operations as well as older, larger mainframe computer systems operations. While these systems differ in size and management, all should be subject to the same general control needs. In addition to discussing general controls procedures, this chapter also discusses some related computer hardware types and characteristics. The aim of this discussion is to encourage internal auditors to ask or look for the correct information in an information systems environment.

18.2 Client-Server and Smaller Systems' General IT Controls

Internal auditors traditionally have had problems evaluating general controls in smaller IT operations, ranging from client-server systems to enterprise desktop systems. These audit control problems arise because smaller systems are often installed with limited staffs in a more "user-friendly" type of environment, while internal auditors typically have looked for general IT controls in terms of the more traditional, larger mainframe IT environment. That is, they are looking for the strong physical security, good revision, and proper separation of duties controls that often do not exist or are only partially implemented in many smaller systems environments. This less formal approach may have been adequate when small business or desktop systems were used primarily for single office accounting or similar low-audit-risk applications. The large capacity and capability of today's smaller systems, the growth of the Internet, and the transition to client-server computing has made these smaller systems important parts of the IT control framework. When evaluating controls in smaller computer systems settings, internal auditors sometimes revert to the traditional, almost cookbook types of controls recommendations. That is, they recommend that desktop systems be placed in locked rooms or that a small, two-person IT development staff should be expanded to four in order to ensure proper separation of duties. While there may be situations where such controls are appropriate, often they are not applicable in small business settings. Internal audit can easily lose credibility if its control recommendations are not appropriate to the risks found in smaller setting.

Enterprises today have implemented many networks and systems to support smaller business units or specific departmental computing, or to provide IT for the entire enterprise. Despite their smaller size, these systems often represent significant general control concerns.

This chapter began with a discussion of differences between general, interdependent controls and application controls in larger systems. These differences are equally applicable for smaller, Internet-based systems and client-server configuration

systems. Internal auditors should understand the general controls surrounding smaller computer systems. Adequate general controls are necessary in order to rely on specific application controls.

(a) General Controls for Small Business Systems

Although some internal auditors once thought of small business computers and client-server systems as one generic IT system class (as opposed to larger, mainframe computers), technological changes have introduced significant differences in their control procedures and in related internal audit concerns. Smaller systems can be implemented in a variety of ways, depending on the system configuration and the size of the enterprise. Internal auditors should be able to recognize these differences and develop appropriate general internal control procedures to review their general controls. This section discusses these general controls in terms of small business computer systems, Internet and networked systems, client-server systems controls, and the classic large systems general controls.

Internal auditors may encounter all of these types of smaller computer systems in a single smaller enterprise today. Small business computer systems provide total IT support for a smaller business function or unit; these systems also may support unit or departmental computing functions in a larger enterprise as part of their central computer systems resources.

Client-server systems are often a combination of various types and sizes of interconnected computer systems and may be found in many enterprises. Process or non-business systems include the numerous types of small computers used increasingly for manufacturing, distribution, and other operational control applications. Internal audit frequently find these specialized control machines in enterprise operations.

(i) SMALL BUSINESS COMPUTER SYSTEM CONTROLS If an IT system is located in a secure facility, has a multitask operating system, or has a relative large application support staff, internal audit should probably consider it to be a "larger" computer system for purposes of audit planning and should review to ensure that the system has appropriate larger-system general control procedures. While not particularly precise, this definition covers the typical major IT system. This same type of attribute-based description can be more difficult in the smaller system environment. A strict computer hardware architecture definition often does not help internal audit decide when to apply smaller-system internal control review procedures. For example, smaller desktop computers can be coupled together with attached peripheral devices to provide more computer power than many traditional mainframe machines. When reviewing controls in such an environment, internal audit should consider these linked computers to be the same as the larger, legacy mainframe systems discussed later in this chapter. Another problem in identifying a smaller computer is that they often look like larger processors. For example, IBM's System i was first implemented in the 1988 as a small business computer called the AS/400. This product line and the individual machine capacities have been expanded many times; many of these systems effectively operate as classic mainframe systems.

Smaller systems, which once were known as minicomputers, have been used for business applications since about the late 1960s. They are a product of the increased miniaturization of electronic components as well as of different approaches used by computer engineers. Because they were relatively inexpensive and easy to use, and

did not require elaborate power or air-conditioning support, minicomputers were once used by many smaller business enterprises as well as for specialized IT applications. Long before the introduction of today's desktop systems, minicomputers brought IT capabilities to enterprises that could not afford the large investments required by classic mainframe systems.

Today's desktop or laptop systems have had a rapid growth curve. Starting with hobbyists building their own microcomputers using newly available integrated circuit chips in the mid-1970s, things really got started in the late 1970s when Apple Computer Corporation was formed and produced the Apple II microcomputer. Although many initially viewed the machine as a curious toy, a spreadsheet software package, VISICALC, introduced about a year later, made the Apple II a serious tool for business decision making. Several years later, in the early 1980s, IBM introduced its personal computer and legitimized the microcomputer as a serious business-processing tool. Today, many machines are said to be "IBM compatible" even though IBM only has its name on some products and no longer manufacturers them.

Today, personal computers, often connected into networks, are used for many business IT applications. Often they are the only computer system resource for a smaller enterprise, and have replaced smaller "mainframe" systems. They may also be used for specialized departmental computing, even though an enterprise may also have a larger, mainframe computer capability. In particular, these specialized computers are used for such applications as research laboratory or manufacturing process control rather than for pure business IT. These same machines may be used for some business-processing applications in addition to their intended specialized purposes.

Ever-increasing speed and capacity have done much to promote the use of these server systems. When the first Apple II was released, it had an internal memory of 42k, or 42,000 memory locations. By the mid-1990s, by contrast, off-the-shelf machines typically came with 32 million memory locations, or 32 mg. Today, they have much larger capabilities by virtually every measure, whether processing speed, the ability to run multiple tasks, or their memory capacity.

These smaller business unit systems sometimes cause difficulties for internal auditors who tell their audit committees that they plan to review the general controls surrounding "all" IT enterprise systems. Clearly, this type of objective covers mainframe and freestanding divisional server systems. Such a planned objective may also cover the enterprise's departmental desktop systems, sometimes freestanding but more often connected to the Internet. However, internal audit's planned reviews often miss such systems as the specialized IT workstations in the engineering laboratory used for recording test results or systems at the end of the distribution line that weigh packages and routes them to the correct shipping dock. These IT review scope ambiguities will only get worse as embedded systems play a greater role in controlling business processes. Embedded systems are the computers that reside behind the dashboard of a car, on the control panel of a video recorder, or even in the kitchen microwave. As consumers, we press these flat-panel screens and generally do not think we are submitting computer system commands. However, embedded systems will take on greater roles in business processes as their capacities and applications increase.

Internal audit's reviews should emphasize the computer systems used for *business IT* purposes. To follow the preceding example, the processor at the end of the distribution line probably uses a standard set of embedded software that cannot be modified by local staff. Very possibly the software was purchased from an outside

systems vendor and, after initial installation and testing, it simply works, with no programmer interaction. Such a machine generally has limited business or control risk implications and is of little or no internal auditor concern.

Internal audit often works in environments where only smaller business systems are used, particularly when enterprises are relatively small. An example would be a not-for-profit enterprise whose only IT resources are a server and desktop systems to support direct mailing and limited accounting-related applications. Internal audit should review general controls over such a server system as if it were a classic, larger enterprise system. That is, there is still a need for systems security, integrity, and backup procedures. These types of smaller business systems generally have these common characteristics:

- **Limited IT staff.** The small business computer system, whether a single desktop system or a series of units tied to a server, will have a very limited dedicated IT staff, if any. A desktop system to provide accounting reports for a small company may be maintained by a single person. A small business or server system may have a manager/administrator and perhaps one or two systems administrators as its total IT department. Such a small IT operation creates a control risk because it is dependent on some separate small consulting firm for much of their IT support, and functions such as backing up critical files may be ignored. However, a small staff size will not in itself create internal controls concerns. Internal audit should be able to look for compensating controls just as it does when reviewing a smaller accounting department that lacks a classic separation of duties.
- **Limited programming capability.** The typical small business computer system makes extensive use of purchased software packages. The enterprise's only "programming" responsibilities may be for updating the software purchased packages, maintaining systems parameter tables, and writing simple retrieval programs. If internal audit finds a larger programming staff or extensive in-house development activity, it should consider employing some of the control procedures discussed in later sections for larger systems-development functions.
- **Limited environmental controls.** Small business systems generally can be plugged into normal power systems and operate within a fairly wide range of temperatures. Because of these limited environmental requirements, sometimes they are installed without important, easy-to-install environmental controls, such as backup drives or electrical power surge protectors. While some small business computer installations or file servers may be housed in formal, environmentally controlled computer rooms, this is not a necessary attribute of such systems.
- **Limited physical security controls.** Because fewer environmental controls are needed, these systems are often installed directly in office areas. The level of auditor concern regarding physical security controls depends on the type of equipment and the applications processed. Internal audit sometimes may recommend that physical security be improved, particularly where critical applications are being processed. In many other instances, however, this lack of physical security controls should not present a significant internal control problem.
- **Extensive telecommunications network.** Virtually all desktop systems today are tied to the Internet. Data and applications can be easily uploaded or downloaded. In addition, materials can be downloaded through common, easy-to-use USB devices. A combination of controls and policies should be established to protect the enterprise.

These characteristics certainly do not *define* a smaller business computer system but merely explain some common attributes. However, they should help internal audit to decide on the control procedures to be used. As noted, when in doubt, internal audit should consider the system to be a larger, more complex one.

(ii) CLIENT-SERVER COMPUTER SYSTEMS The term *client-server* first appeared in IT literature in the late 1980s. To non-IT specialists, including many internal auditors, it is one of those specialized IT terms that is often difficult to understand, let alone describe. However, client-server architecture has become a very popular IT configuration in all sizes of enterprises and systems. In a local network environment, for example, each of the workstations is a *client*. A centralized processor, which contains common shared files and other resources, is called the *server*. There may also be specialized servers for such tasks as storage management or printing. Workstation users submit requests from client machines to a server, which then provides support, or serves, that client by doing the necessary processing.

This client-server architecture, however, goes beyond just a workstation and a server. An application that queries a centralized database can be considered the client while the database that develops the view of the database is the server to all workstations requesting database service. Similarly, an application program can request services from an operating system communications server. Exhibit 18.1 shows

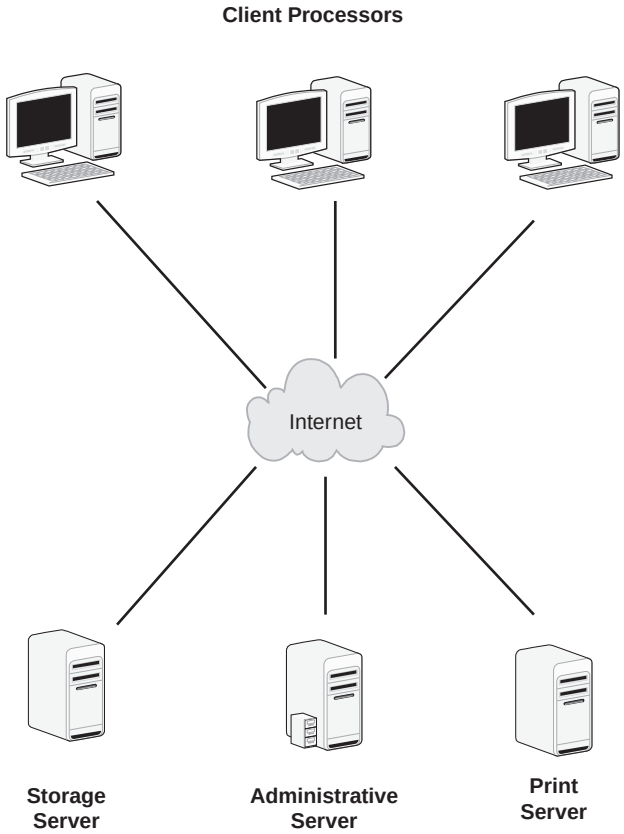


EXHIBIT 18.1 Client-Server System Configuration

a client-server system sample configuration where a single server handles requests from multiple clients across a network. This client-server configuration, though very general, represents the typical IT system of today.

(iii) NONBUSINESS SPECIALIZED PROCESSOR COMPUTER SYSTEMS In many enterprises today, other systems can be found in areas beyond IT operations such as engineering laboratories, manufacturing control operations, marketing departments, and elsewhere. These systems may be used for process control, automated design work, statistical analysis processing, or many other applications. Some are totally dedicated to specific applications; others may be used for a variety of tasks within their assigned functions. This multitude of IT machines has come about in many enterprises because of the relatively low cost of such machines and the familiarity of many professionals with IT techniques, and because of the inability of traditional IT departments to support specialized IT needs.

Although these systems are not used for traditional business information needs, such as maintaining accounts receivable records, they often support critical applications for the enterprise. For example, an engineering computer may support new product computer-aided design (CAD) work. Systems backup and integrity concerns in this environment may be as great as in the typical business IT center. Internal audit's role in regard to specialized IT operations will vary with both management's direction and internal audit's review objectives. While some audit enterprises will have little involvement with reviews over specialized computer systems, IT controls reviewed here often play an important role in support of internal audit's understanding of control procedures and in other operational audit activities.

Before attempting any review of such a specialized computer system, internal audit should obtain a rough familiarity with the functions of that operation. For example, an internal auditor who plans to review a dedicated computer-aided design and manufacturing (CAD/CAM) computer operation needs a general understanding of the terminology, general workings, and objectives of CAD/CAM.

Reviews of specialized IT systems are not recommended for the less experienced internal auditor. In order to find control analogies from normal business IT situations and translate them to specialized controls environments, an auditor must be fairly experienced in reviewing business IT computer centers, whether larger or smaller operations. Over time, internal audit will encounter more of these specialized computer operations. The creative internal auditor can make increasing contributions to management by performing operational reviews over these computer centers on a periodic basis.

(b) Smaller Systems' IT Operations Internal Controls

As discussed, internal auditors have traditionally looked for a proper separation of duties as a first procedure for evaluating IT general controls. This control, however, is also often lacking in a smaller business IT function. While good IT control objectives call for a proper separation of responsibilities between users and operators, these controls are often difficult to establish in a small department. When internal auditors first reviewed general controls in smaller IT departments and tried to apply traditional large-system control remedies, their recommendations were hard to sell to a cost-conscious management.

The responsible manager for smaller client-server systems today may also be the principal technical specialist and operate the equipment for such tasks as backup processing. Separation of duties controls found in a larger shop does not exist in this smaller environment, but there should be compensating controls, including:

- **Purchased software.** Nearly all smaller computer systems today operate with purchased software packages where "programmers" do not have access or have very limited access to source code. A major task may be to install vendor software upgrades on the local system.
- **Increased management attention.** Although small business enterprise managers may have very little knowledge of IT techniques, they often give considerable attention to the key computer-generated reports. In a small company, it is not unusual for top management to review, for example, an accounts receivable aged trial balance in detail and on a regular basis.
- **Separation of input and processing duties.** In virtually all modern small business computer systems today, users submit data inputs through their individual workstations and receive outputs on their terminals or remote printers.

Even with these compensating controls in modern, small business IT systems, internal audit should also be aware of potential control risks and weaknesses. There still exist IT departments in which the responsible manager implements many of the applications, has responsibility for the network management, controls all passwords, and appears to be the only person in the enterprise who understands the IT applications. While a limited staff may be acceptable in some circumstances, the enterprise faces a risk if all IT knowledge is vested in only one person. Other control weakness symptoms in the smaller IT enterprise that do not typically exist in the larger department include:

- "Loyal" employees who do not take their vacations or time off
- The use of special, undocumented programs known only to the IT manager
- Direct IT department participation in system input transactions, such as adjustments to the inventory system

Control risk may be a major consideration when audit procedures have identified significant control weaknesses in these smaller business systems. In larger enterprises, internal auditors often look for documented position descriptions as evidence of good management controls over the IT function. However, some smaller enterprises do not even have such descriptions for *any* employee. An internal auditor will not be effective in suggesting that such position descriptions be drafted just for the IT function while ignoring the rest of the enterprise.

As discussed, a plan of organization and related position descriptions that define responsibilities are often among the strongest control procedures in a larger IT enterprise. The size and informality typically associated with smaller enterprises tends to weaken controls. Senior management should have a good understanding of the IT function, its plans, and its objectives. A very important general control for the smaller IT enterprise is adequate documentation over systems and procedures. There have been instances where both members of a two-person IT enterprise suddenly resigned due to a disagreement or better employment offer. Without adequate documentation, it is very difficult for someone else to take over. This is true

even if the enterprise primarily runs packaged software, since there may be many special procedures associated with those packages. The risk is equally high if the enterprise uses desktop systems where users do much of their own work. The network administrator who configures the system and backs up files has a key control responsibility.

Sometimes a smaller IT system operation is an operating unit of a larger enterprise with centralized IT facilities. Even though the smaller business unit and its IT operations may be entirely freestanding, it may be subject to corporate standards and procedures. In order to ensure compliance with these standards, internal audit should have a general understanding of them and the level at which these corporate standards are expected to be followed. Sometimes large enterprises issue mandatory standards applicable to all of their operating units, no matter their size, even though some standards may not be fully practical for smaller units. While central management may look the other way regarding local compliance with these standards, internal audit often feels compelled to document any violations. If such problems exist, internal audit should discuss these concerns with the central IT management group responsible for the standards. Little is accomplished if internal audit documents violations of corporate standards at remote units when central management does not expect full compliance. This disparity between corporate and local standards practices may be a topic more for a centralized review of standards.

(c) Auditing IT General Controls for Smaller IT Systems

Some smaller IT systems may be separate operating units of a larger enterprise and provide support for the total enterprise. Such systems may have many of the attributes of a larger, server-based system, including a limited but formal IT enterprise, production schedules, and a responsibility for implementing new applications. However, the smaller IT system enterprise often has no other specialized functions. Internal audit will encounter a variety of computer hardware brands or product names in a smaller systems environment, but most will be open systems with a common operating system that can function no matter what brand of hardware is used. In classic mainframe computers, the manufacturer generally built the computer hardware as well as an operating system. Numerous vendors supply such small business computer systems with both improved functionality and price performance. Internal auditors will be more effective in reviewing small business computer system controls if they have an overall knowledge of some of their capabilities.

Despite the more informal nature of a typical small business computer system, internal audit may expect some of the internal control concerns discussed next.

(i) SMALLER SYSTEM CONTROLS OVER ACCESS TO DATA AND PROGRAMS ARE OFTEN WEAK

When unauthorized persons are allowed to access and modify computer files, general controls are very much weakened. Internal audit should consider access to data and programs to be *the major general controls objective* when reviewing the smaller IT enterprise. This is true whether the IT department uses packaged software products or spreadsheets or databases developed in-house.

Controls over access to data can be considered in terms of both specific applications and general controls. However, in smaller computer systems, general controls often have a greater importance than specific application data access controls.

Small systems, whether a series of laptops connected through a wireless connection or a powerful server system, often do not have the sophisticated security controls

found on many larger mainframe-type systems. Rather, these smaller systems have a user log-on/password identification coupled with menu-based information security. A systems user typically enters the assigned log-on or userid identification code onto the terminal and receives a menu screen with the applications available to that code. The user then can access only the applications assigned to that menu.

These menu-based security systems, historically found in systems like IBM AS/400s, provide a fairly effective control against improper access attempts. However, they can break down due to the informality of many smaller enterprises. Log-on codes are often not changed on a regular basis, one general menu is given to virtually all employees, or terminals with more privileged IDs are left on for virtually all to use. Because users often are not aware of potential data vulnerabilities, management may give only minimal attention to such security issues. In order to review controls in this area, internal audit should first gain a general understanding of the data security system installed, which may range from a good password-based system to a highly structured set of procedures. The next step is to understand how that security system has been implemented and is being used. To do this, the internal auditor should spend some time reviewing how application controls are used in user areas.

A small business computer system may not have the logging mechanisms to monitor invalid access attempts, and audit should review the overall administration procedures covering the security system. These can include reviewing how often log-on codes are changed, who has access to the system administrator's menu, and local management's general understanding and concerns regarding IT access controls.

(ii) UNAUTHORIZED USE OF UTILITY PROGRAMS Modern small systems often are equipped with powerful utility programs that can easily change any application data file. These programs are designed to be used for special problem-solving situations, and they often produce only a limited audit trail report. All too often, these utilities serve as substitutes for normal production update programs or are used by an IT manager for these special updates. Sometimes they even are given to users. For example, an enterprise may have installed an inventory status system. While the system normally provides proper stock-keeping records, the inventory status may become misstated from time to time for a variety of reasons. In order to help users correct these inventory status record-keeping problems, the IT administrator may correct inventory balances by using a utility program. While the IT manager may be following proper management direction in the normal use of such a program, there may be no audit trails over its use.

These utility programs go by a variety of names depending on the type of computer operating system used. For example, in a UNIX operating system environment, the *su* (super-user) command has some powerful attributes that should be protected. Internal audit should understand the types of standard utility programs available for the system under review. An enterprise's usage of these programs can best be determined through inquiry and observation.

(iii) IMPROPER IT DATA AND PROGRAM ACCESS REQUESTS The informality of many smaller enterprises often allows data to be accessed improperly through normal IT operations procedures. For example, someone known to the IT function may initiate a special computer run, which results in improper access to confidential data. In larger, more formal enterprises, often such a request would require special

management permission, but more informal enterprises often waive such requirements. This type of access may be a greater control risk than access through use of improper programs.

Internal audit should look for controls to prevent such casual IT requests. The best control could be a formal "request for data services" type of form, approved by management. In addition, logs should be maintained listing all production IT activities as well as the name of the requester and the report recipient. Many of the control concerns over improper access to data also apply to small system program libraries. Small business systems typically do not have the sophisticated software control tools over program libraries found in larger systems, but they generally do have menu-based systems that offer some security types of controls. Without a proper menu type of security system to limit improper access, often it is relatively easy for someone with a little knowledge to locate and potentially modify program library files.

Internal audit may also find weak controls over program library updates. The one or two IT personnel in a smaller IT department who act as network administrators typically can update program libraries without documenting those changes or obtaining any type of upper management authorization. Some of these changes may be justified in order to respond to user emergency requests, but others may not be. It is difficult, if not impossible, to install separation-of-duties enterprise controls over small business system program libraries. In addition, it probably will not work for internal audit to suggest that management formally review and approve all program library updates—managers will neither be interested in nor have the technical skills to perform such reviews. The best control method here might be to install procedures that require the logging of all changes or software package updates to the production program library, with such logs subject to periodic internal auditor reviews.

IT system update controls can take advantage of the fact that IT systems in many small businesses maintain hash[1] total counts of program sizes in bytes and also can retain some form of date or version number within the program name. Internal audit might then suggest this small business computer system program library control:

- Establish program naming conventions that include the date or version number included with the program name. When not available in commercially purchased software, a separate control file with this data can be established. This feature is becoming increasingly common; for example, it can be implemented within the Windows XP operating systems.
- Have the persons authorized to make program table or parameter changes log in the version number, date, program size, and reason for the change in a manual listing subject to periodic management reviews. If the application was developed in-house, the source code should contain comments explaining the change.
- Maintain at least one backup copy of the program library and rotate a copy of the program library file to a secure portable disc drive in an off-site location at least once per week.
- Strengthen access controls such that nonauthorized personnel cannot easily access program library files.
- Perform an internal audit review of the library change log on a periodic basis. That review should match logged program versions, dates, and sizes with data reported on the program library file.

These steps will not provide internal audit with complete assurance that all program changes have been authorized; however, if internal audit periodically reviews logged changes and questions any discrepancies, programmers probably will take care to document and log any production program changes.

The point of this section is that there are or should be some general IT internal control concerns for all smaller systems, whether they are a network of laptops coupled to a server over wireless links or a freestanding office desktop system. Exhibit 18.2 contains general control objectives for reviews of smaller business IT systems.

EXHIBIT 18.2 General Control Objectives for Smaller Business IT Systems

1. Determine if there is a complete and current inventory of systems hardware, including servers, printers, and network controllers, as well as a complete inventory of application and systems software.
2. The network hardware inventory report should contain model and identification numbers. Review a limited sample of these items to determine the equipment is installed as described.
3. Trace a sample of the listed application and systems software to determine that current versions are installed, that appropriate documentation is in place, and that vendor licenses are current.
4. Review file and data backup procedures and determine that these data are regularly backed up to secure locations.
5. Observe computer server facilities and verify the equipment is located in limited-access secure facilities with adequate power and environmental controls.
6. Observe storage processes for backups of key files to determine that media are regularly backed up to secure off-site locations.
7. Assess the adequacy of access control security procedures to determine that key systems and files are adequately protected by passwords that are regularly changed.
8. Review procedures in place for restricting, identifying, and reporting on unauthorized users of the network environment, and assess the adequacy of processes to investigate and correct security violations.
9. Assess the adequacy of systems security monitoring processes as well as new employee training practices in place to emphasize application security.
10. Review the adequacy of procedures for installing new software in the systems environment, and assess that controls are in place to prevent the introduction of unauthorized software products.
11. Review a sample of key applications and verify that they are supported by adequate continuity plans for disaster recovery purposes. Also, determine that continuity plans are tested periodically.
12. Interview persons responsible for network security to determine that adequate firewall tools have been installed.
13. Review records of systems downtime over a recent period, and determine that adequate short- and long-range measures are in place for continual improvements.
14. If available, obtain application operating schedules covering key financial and operational applications, and determine that adequate attention is given to application internal controls.
15. Interview the systems manager/administrator to assess whether this person is knowledgeable and properly trained. Also, if the system is managed by outside consultants, review the adequacy of systems support efforts.
16. Interview a sample of systems users and determine if they are satisfied with systems performance, including response times and availability.

18.3 Components and Controls of Mainframe and Legacy Systems

The UNIVAC II, one of the first successful business IT computers, was introduced in 1951 and helped predict the results of the 1952 U.S. presidential election. It required a huge amount of physical space, weighed 15 tons, and cost $1.3 million (in 1950 dollars). Its central processing unit (CPU) was housed in a cabinet with doors on both ends so a technician could walk through it to make any required repairs. A "bug" in those days referred to an insect that got into the CPU cabinet and perhaps blocked a relay tab. Today's $500 personal computer system has at least 50,000 times the memory and speed of the UNIVAC II—or more. Was the UNIVAC II a "large" computer system? In today's terms, although it was large, based on its cost or the floor space it occupied, with respect to its memory, speed, and functional capabilities, the answer is no. The term *large* as it applies to computer systems becomes even more difficult today. Although IT professionals once called these smaller systems "minicomputers," those same systems today may appear to be "large computers" to an internal auditor because they operate as servers to support a large variety of IT equipment, such as multiple workstations, disk and storage devices, and many other devices. The large system computer hardware may be supported by a big operations staff and will handle many varied processing tasks. Different employees each have their own definitions for a larger computer system. For example, the technical programmer may define a larger computer system in terms of the central processor's internal design or architecture. Management may define the same computer system's relative size in terms of what the equipment cost and the size of the IT staff necessary to support it. Some auditors not familiar with computer systems may consider an older legacy computer system, located inside a secure facility with a raised floor, to be large. This is particularly true if the auditor's experience is limited to small laptops, desktop, or server machines.

Internal auditors once were more interested in the size of the computer system to be reviewed because of their impact on internal audit's control review procedures. This has changed with the introduction of many new technology developments. Today there is no longer a direct relationship between machine size and its audit complexity. Nevertheless, some of the controls that internal audit would expect to find in a very large computer center operation would not necessarily apply to the small business computer system discussed earlier. For example, a technical or systems programming staff, responsible for monitoring performance and maintaining a larger computer's operating systems, is often not necessary for a smaller and more modern computer system.

(a) Characteristics of Larger IT Systems

Larger IT systems usually have some common characteristics, whether they are classic IBM mainframes requiring a chilled-water cooling or several interconnected UNIX file server processors. While all IT internal control characteristics may not apply to every larger computer system, these characteristics are typical of larger business IT systems:

- **Physical security controls.** A larger computer center with significant data files is usually located in a room with locked access controls and no windows to the outside. This security helps to protect the equipment as well as the programs

and data. Locked doors to the computer room prevent unauthorized persons, both employees and outsiders, from entering the area to pick up reports, to ask distracting questions of the operators, or to cause malicious damage.

While all business operations are subject to terrorism, fires, or floods, a larger system computer center has a particular vulnerability because the equipment cannot easily handle these stresses. Because of the type and extent of data processed in the modern larger-scale computer system, systems operations should be located in guarded and protected locations and built to minimize exposure to fires, floods, or other acts of God.

- **Environmental control requirements.** Specialized electrical power systems as well as dedicated air conditioning or water-cooling chiller systems are often necessary because miniature electrical components operating at full power generate a considerable amount of heat. Because of these special needs and because computer systems consist of multiple pieces of equipment connected by communications cables, the IT hardware is located in specialized rooms with dedicated environment monitoring controls and false floors that provide space for power cables and ventilation. Larger systems, vulnerable to electrical power outages or fluctuations, are almost always equipped with emergency power supplies that can smooth out power fluctuations or provide a source of emergency power to allow the computer system an orderly shutdown.

  Some systems may even be supported by independent generators to provide power over an extended period in the event of an outage. Weaknesses in environmental controls can result in failures in the operation of key IT applications. Internal audit should always be aware of control procedures in this area and make recommendations where appropriate.
- **Separate storage media libraries.** The storage or library areas for magnetic cartridges and tapes are typically adjacent to the computer equipment rather than in the machine area to provide extra protection and more efficient mounting and backup of tape cartridges. Automated tools are often used to schedule and call up cartridges for mounting as well as to write internal labels onto tape files and to schedule them for backup rotation. Earlier generations of magnetic media files were often rotated to another library storage facility so that, in the event of a fire or other disaster within the computer room facility, they could be recovered for transfer to an emergency backup processing site.
- **Multitask operating systems.** Virtually all computers use some type of a master program or operating system to control the various programs run by the computer and other tasks, such as reading disk files or supplying report data to print server facilities. Typically, these operating systems can run many programs in parallel and perform other tasks, such as printing. Managing a multitask operating system on a larger computer usually requires specialized personnel, called systems programmers.
- **In-house programming capabilities.** While smaller staff enterprises typically purchase the majority of their applications from software vendors or have their systems supplied by an enterprise headquarters staff, enterprises with larger computer systems are often supported by an in-house systems and programming department ranging in size up to several hundred or more employees. Programmers are different as well. Until the early 1990s, many used the COBOL language. Today many may only develop parameters for specialized purchased software packages or do some custom work in languages such as C++ or Visual

BASIC. In-house programmers almost never write custom inventory control or payroll applications. A larger enterprise with its own programming and systems analysis staff should have a fairly formal systems development methodology (SDM) or system development life cycle (SDLC) procedures, to develop and implement new applications. SDLCs are discussed in Chapter 30. There should be specialized library files to control computer programs as well as technical documentation covering the programmers' work.

- **Extensive telecommunications network.** Virtually all modern systems have an extensive telecommunications network to support multiple online terminals, located throughout the enterprise, and connected either directly to the central computer system or to the Internet. The network may also require specialized technical personnel within the IT enterprise to manage telecommunications.
- **Very large or critical files** Although a computer system may be rather small in many respects, one or more applications may maintain critical data on very large databases. While these critical files once consisted of many reels of magnetic tape, electronic database management systems are used today. Because of the criticality of such large databases, the IT system—whatever its actual hardware configuration—takes on characteristics of a larger system. The need for backup copies and the integrity of critical files is crucial to the IT function to help ensure the accuracy, integrity, and completeness of the database.
- **Input-output control sections.** Although almost unknown today, some IT systems had an input-output control functions to receive any batch input data (such as tapes mailed from remote sources), to distribute any inputs, and to schedule and set up production jobs. In the earlier days of IT, when most production jobs were run in a batch mode, such control functions often balanced input batches to system outputs and resolved many problems. Today, users generally take responsibility for their own data, which they submit through terminals in user areas with outputs transmitted back to them.

These characteristics, although not specific to larger legacy systems, provide some guidance to help determine whether an internal auditor is working with a larger IT system environment. There are many variations in what can be defined as larger or smaller computer systems. While internal audit's control objectives will remain essentially the same for both, control procedures will differ. Techniques for auditing smaller systems were discussed in Section 18.2. If an internal auditor does not know whether to consider a system a large or a small system, the safest approach is to consider it to be a larger, more complex one.

(b) Classic Mainframe or Legacy Computer Systems

Larger IT systems typically have their own unique control characteristics. Although much as been published about today's client-server and desktop systems, significant changes have also taken place over the years for larger, mainframe computer operations. For internal auditors, internal controls issues that were once frequent audit concerns are now an almost accepted part of operating procedures for large computer systems. Other, newer control issues have become part of the internal audit's review process. In the early days of mainframe computer systems, a common internal audit concern was that computer operators should neither have access to

computer operating programs nor the knowledge to change them. The reasoning was that if programmers were allowed to operate the IT equipment, they could potentially improperly modify or run unauthorized programs. Checklists and audit programs were published—including earlier editions of this book—that directed auditors to attest that, among other matters, computer operators did not execute programs and programmers did not operate the equipment. Because of the complexities of modern, large IT operating systems and the high production demands within the machine room today, this separation of duties generally exists in the larger enterprise but is still a concern in the smaller enterprise or computer systems environment, as discussed in Section 18.2. Of course, internal audit should always confirm there is an adequate separation of responsibilities within any IT function.

There is no typical hardware configuration for the modern larger IT enterprise. Often inexperienced auditors tour through a room filled with central processors, servers, storage devices, and other equipment with little understanding of what is being seen. Because of the miniaturization of electronic components, the modern computer center takes much less space than was previously required. In addition, there have been significant changes in the design of many IT peripheral components. The once-common magnetic tape drives, for example, now have been all but replaced by much smaller cartridges that have a much higher capacity. Disk drives are configured as arrays of smaller discs with considerably greater data storage capacity. Some output printing is still done on remote high-speed laser printers, but enterprises increasingly have gone paperless and communicate reports to digital files. An internal auditor should gain an understanding of the types of IT equipment used by requesting a hardware configuration chart from operations management. While internal audit typically will not be in a position to determine, for example, the correct models of disk drives, such a chart will indicate that management has done some planning in the computer hardware configuration. These charts are often filled with model numbers rather than explanations of the equipment. The internal auditor should always ask questions about the nature of this equipment.

While the number and type of tape drives, printers, and other equipment will vary, an internal auditor can expect to find similar characteristics in all operating facilities. These similarities should help internal audit to develop procedures to test the appropriate controls. When auditors first started to review IT general controls, they often looked for such things as locked computer room doors, fire extinguishers, and proper batch controls. These controls are now in place as a matter of course in larger computer centers. While internal audit should always keep them in mind, other general control objectives and procedures must also be considered.

(c) Operating Systems Software

Early business computer systems had little more than a single basic master program—what came to be called an operating system—to load and schedule application programs, with those application programs taking care of their own utility functions, such as tape file label checking or sorting data. The IBM 1401 computer of the mid-1960s had only 8K (8,000 bytes) of memory to hold its operating system. The basic 1401 operating system did little more than load programs and communicate with input and output devices. Modern operating systems software is much more complex and capable of handling many users and systems functions. The characteristics of

systems software that an internal auditor will encounter in a larger, legacy computer system include:

Operating systems software. IT operating systems are the basic software tools that provide interfaces among systems users, application programs, and other IT hardware. In addition to the basic operating system, an internal auditor will encounter various monitors and controllers, including specialized software to schedule jobs or handle logical security. Operating systems software includes the central operating system, control programs, various programming aids, and application-related support software.

An internal auditor should develop a high-level, general understanding of the various types of installed operating systems software that may be on a given system as well as the associated control characteristics, including:

- **Central operating systems.** The operating system (O/S) supervises the processing of all systems resources and programs. IBM's older large MVS operating system is an example. Because these operating systems often were tied so closely to the hardware they control, operating systems traditionally have been unique to the computer vendor's equipment. Today, the trend is toward common or open operating systems. The UNIX operating system, for example, has been implemented on virtually all sizes and models of computer systems. Although it is less common on larger mainframes, UNIX is found on many small to midsize computers and is a major controller for Internet systems. UNIX provides common user interface functions with the hardware where it is installed. Various versions of UNIX differ slightly from one another. In addition, the open source operating system, LINUX, is becoming increasingly common today.
- **System monitors.** A variety of basic operating system support software products help schedule jobs, monitor systems activities, and help solve operator problems or system errors. These products are tied very closely to the basic operating system but usually are sold and installed separately. Monitors provide internal signals to other operating system functions (i.e., they are similar to a semaphore signal once found on a railroad track). Once a train enters a stretch of track, a control monitor detects the train and raises various semaphores to signal other trains that one is already on the track. Some monitors just log operating system activity for historical purposes. An example is IBM's legacy system SMF (system maintenance facility) utility, which monitors virtually all systems activities, including which programs are processed and the various disk files used. Operating systems memory dumps are another example of a monitor. Here, the contents of the affected system memory are reported when a program goes into an error status.
- **Network controllers and teleprocessing monitors.** These specialized operating system programs supervise and control transmissions between the host computer system and peripheral devices. These devices allow the applications processing on a host computer system to communicate with multiple network connections. Software programs that support the interaction between online terminals and the host computer also fall into this class of operating software. IBM's online monitor—often called "kicks," or

the CICS (Customer Information Control System)—allows user terminals to access and process online programs. An internal auditor may find the name CICS somewhat curious as it is generally used for much more than customer information applications. CICS was originally developed by IBM in the days of its old 360 series computers for a specific customer that needed a method to access programs in an online manner. IBM did not have such an online software product at the time, although its mainframe computer system competition did. CICS, the special product IBM created, has since become IBM's basic online processing control product; many have forgotten what the acronym CICS really means.

All of these special names can cause an auditor some communications problems. Computer systems users may know what the product does but may forget what the acronym really represents. As long as the systems specialist and the auditor understand the functions of a software product, there is little need to worry about the specific meaning of the acronym. Internal auditors should not become discouraged by this "foreign language" of specialized computer software terms and names. When IT technical personnel speak in their own techno-jargon, an internal auditor should always ask for clarifications.

18.4 Legacy System General Controls Reviews

In an older, traditional IT environment, the computer operations area was often internal audit's prime area of internal control concern. In those days, computer operators had considerable power to make changes or to bypass systems controls, such as overriding data file label controls, making changes to program processing sequences, or inserting unauthorized program instructions into production applications. While still possible today, both the complexity of large computer operating systems and the sheer volume of work passing through the modern IT operations center make these unauthorized actions difficult. Internal audit has greater risks to consider.

Many once-common internal audit IT operations control improvement recommendations are no longer feasible today. For example, older business data center computers had a console printer attached to record operator commands. Internal auditors traditionally recommended that these console logs be reviewed on a regular basis. These logs were often ignored but were useful for tracing inappropriate operator activities. Today, this console activity is recorded onto log files, but the sheer volume of that data makes a periodic human review of console log reports all but totally unrealistic; other tools and controls are available to help internal auditors understand operations controls. Internal audit should initially gain an understanding of the information system enterprise, its established control procedures, and specialized duties and responsibilities.

An important step in an internal audit review of IT operations larger system general controls is to define clearly that review's objectives. All too often, management may ask internal audit to "review the computer systems controls" in the data center. Memories do not fade very fast; that request may be based on IT controls as they

once existed in older systems. An internal auditor should consider these questions when planning the review:

- What is the purpose of the information system operations review?
- Which specific controls and procedures are expected to be in place?
- How can evidence be gathered to determine if controls work?

Based on the results of this exercise, internal audit should develop a set of control objectives specifically tailored for the planned review rather than just use a standard set of internal control questions. The internal audit objectives identified depend on the purpose of the review.

If management has requested a review of the costs and efficiency of data center operations, for example, internal audit procedures might include such areas as the chargeback and the job-scheduling systems. Although a larger system IT general controls review can have a variety of purposes, it often fits into one of four review types:

1. **Preliminary reviews of IT general controls.** Outside auditors sometimes call this type of review a *preliminary survey* or an *assessment of control risk*. Its purpose is to gain a general understanding or overview of the IT controls environment. Internal audit asks questions, observes operations, and reviews documentation, but there is typically only very limited testing, if any. For example, internal audit might inquire about the procedures for updating production program libraries and might review the forms used for the approval process. However, an internal auditor probably would not select a sample of the programs in the production library to determine if those selected programs had followed proper library update procedures.

   A preliminary review can help determine the need for a more detailed general controls review or extended control risk assessment at a later date, or can gather preliminary controls information for a specific applications review. This type of review is limited in scope and may not cover all aspects of the IT enterprise. Some areas where a preliminary review would be appropriate might include an internal controls review of IT operations at a new acquisition or a follow-up review after a very detailed general controls review from an earlier period; the review here would emphasize changes in control procedures as well as actions taken on prior audit recommendations

   Although there can be many changes based on the review's specific purpose, Exhibit 18.3 outlines steps for a preliminary survey of IT general controls. These steps should guide an internal auditor to gain information about the general structure of IT operations, how the IT function plans and organizes resources, its management reporting tools, and procedures for security and contingency planning. These audit steps will not help in understanding the types of applications in place but will assess how that IT function is organized and managed.
2. **Detailed general controls reviews of IT operations.** A comprehensive, detailed review of IT larger systems general controls should cover all aspects of IT operations, including systems programming, telecommunications controls, and storage administration. A detailed general controls review, including tests of controls, often requires internal audit to spend considerable fieldwork time

EXHIBIT 18.3 IT General Controls Preliminary Survey

1. Obtain basic information about the environment through initial exploratory discussions with information systems (IS) management.
2. Review the organizational chart to determine that appropriate separation of functions exists. Discuss any potential conflicts with IS management.
3. Obtain job descriptions of key IS personnel, and review them for adequate and appropriate qualifications, task definitions, and responsibilities. Ensure that security and control accountability are appropriately assigned to key personnel.
4. Based on discussion within management both inside and outside the IS organization, assess whether the organizational structure is aligned with business strategies to ensure expected IS service delivery.
5. Review IS policies and selected procedures for completeness and relevance with specific emphasis on security, business continuity planning, operations, and new systems development.
6. Inquire whether responsibilities have been assigned to keep the policies and procedures current, to educate/communicate them to staff members, and to monitor compliance with them.
7. Based on discussions with senior IS management, assess whether strategic, operational, and tactical IS plans are in place to ensure alignment with the organization's overall business plans.
8. Determine whether an IS steering committee exists, and review this committee's functions through a limited review of steering committee meeting minutes.
9. Ensure that a formal methodology is used in the development of new systems or major enhancements to systems in production. The methodology should include formal steps for definition, feasibility assessment, design, construction, testing, and implementation as well as formal approvals at every stage.
10. Assess the uses of system development efficiency and effectiveness tools, including joint application design (JAD), rapid application design (RAD), code generators, CASE tools, and documentation generators.
11. Determine that a process is in place for making changes to application programs in production, including testing and documentation sign-off, and formal approvals to implement the change.
12. Ensure that responsibility for physical and logical security has been appropriately apportioned and that appropriate documented procedures exist.
13. Review procedures in place for operating and maintaining the network, in terms of device configuration and software parameter changes, and ensure that procedures for allocating and maintaining the network configuration are performed on a scheduled basis and under proper change management.
14. Review the business continuity plan to ensure that detailed plans for recovery of operations have been prepared and that the plans are documented, communicated to the appropriate personnel, and properly tested on a periodic basis.
15. Review both the IS budget and the actual costs as well as performance against those measured to assess financial performance. Discuss the reasons for any variances.

in both the IT operations and development functions. While the preliminary review sometimes can be performed by a less experienced auditor who is developing IT audit skills, a detailed general controls review is best performed by more senior audit staff members with a good understanding of IT controls and procedures.

Based on a preliminary IT operations walk-through review, internal audit should develop an understanding of the control procedures over IT operations.

The detailed audit procedures performed can be modified based on this preliminary information. Questions internal audit might pose could include:

- **How is work scheduled?** Some larger system computer operators do little more than initiate jobs from a production job queue file, while others have considerable authority in deciding which jobs to run. In the latter situation, internal audit might want to spend time reviewing control log reports and operator instructions. If these procedures have been automated, internal audit may want to consider a specialized review of the production control software area.
- **How is storage media managed?** Automated tools are often used here. In addition, some operations have a separate library facility where production media cartridges are mounted. Even when software has been installed, computer operators often can bypass label controls and introduce incorrect files into a production environment.
- **What types of operator procedures or instructions are used?** Operations documentation in larger systems can take a variety of formats; internal audit should have a general understanding of this documentation format and content to help in the design of specific audit tests.
- **How is work initiated, and how does it flo through operations?** In many larger computer systems operations, production is initiated through remote job entry user terminals. In others, the production-control function funnels all necessary input data to machine operations. Some functions rely on users to initiate most inputs through their online terminals. The type and nature of internal audit's tests will depend on the customary procedures.

The basic idea is for internal audit to understand how IT operations function. The effective internal auditor should go through a set of these types of questions prior to each review. A large systems operations function may install new procedures from time to time, changing or adding complexities to the control structure. The audit procedures to be performed in a detailed review of general controls for a legacy computer system can be extensive, depending on the size and scope of the audit. Exhibit 18.4 contains a limited set of control objectives for this type of review.

3. **Specialized or limited-scope reviews.** Because of management requests and perceived risks, auditors often perform limited reviews over specialized areas within an overall IT function. These specialized reviews can be limited to one function, such as database administration, or a specialty area, such as output report distribution. Often management will request that internal audit perform this type of a review due to some identified problem, such as a well-publicized security violation.

   Often considerable internal auditor creativity is required to review a highly specialized or technical area of IT operations. Management may be concerned about the equity of the computer chargeback system and may ask the audit department to look at it. Internal audit will need to gain a general understanding of the system used, spend time planning the additional procedures and tests to be performed, and then return to the actual testing.

   As IT has grown in complexity and importance to the enterprise, auditors can expect to perform more of these specialized, limited reviews. With the IT function a major resource in many enterprises, it may be inappropriate to attempt to review *all* IT general controls in *all* operational areas as one single

EXHIBIT 18.4 Large System IT General Controls Objectives

1. Determine that the computer equipment is located in a secure, environmentally controlled facility.
2. Discuss physical and environmental control procedures with information systems management to determine current policies and future plans.
3. Tour computer operations facilities, and observe physical security strengths and weaknesses, including:
   a. The existence of locking mechanisms to limit computer room access only to authorized individuals
   b. The placement of computer room perimeter walls and windows to limit access
   c. The location of power transformers, water chiller units if appropriate, and air-conditioning units to provide proper protection
   d. The general location of the computer room facilities within the overall building to minimize traffic
   e. The existence of fire detection equipment, including zone-controlled heat and smoke detectors
   f. The existence of a zone-controlled, overall fire protection system, including local extinguishers
4. Review computer room temperature, humidity, and other environmental controls and assess their adequacy.
5. Briefly review maintenance records to ascertain that physical and environmental controls are regularly inspected and maintained.
6. Ensure that production processing is scheduled to promote efficient use of computer equipment consistent with the requirements of systems users. Through interviews with operations management, develop an overall understanding of computer processing demands, including online and batch production work as well as any end-user computing.
7. Also through interviews, describe the telecommunications network surrounding the computer system, including connections to workstations, computer centers, and the outside.
8. Review procedures for scheduling regular production jobs, including the use of automated job-scheduling tools.
9. Match a limited number of scheduled production jobs against actual completion times to determine whether actual schedules are followed.
10. Determine that operating system job classes or priority codes are used to give proper priority to critical production jobs, and evaluate procedures for rush or rerun jobs.
11. Review documentation standards for production applications to determine that they provide operators with information regarding:
    a. Normal operations, including instructions for special forms, tape files, and report disposition
    b. Application restart and recovery procedures
12. Review procedures, automated or manual, for turning new applications or revisions over to production to determine if there is a review by operations following standards.
13. Determine that policies prohibit computer operations personnel from performing programming tasks or running unauthorized jobs.
14. Determine that production source libraries cannot be accessed by operations personnel.
15. Assess information systems procedures for periodically reviewing the contents of log files or otherwise monitoring improper operator use of computer equipment.
16. Review and document procedures for changing production programs or procedure libraries when emergency situations require special handling.
17. Determine that all emergency processing activities are properly documented and are subject to subsequent management review.

(*Continued*)

EXHIBIT 18.4 Large System IT General Controls Objectives (*Continued*)

18. Select several documented emergency program fixes and determine that the necessary changes were added to production processing libraries and were documented.
19. Determine that an automated system is in place to log all computer systems activity, including all jobs and programs run, any reruns, abnormal terminations, or operator commands and data entered through system consoles.
20. Determine that computer activity logs are reviewed periodically, that exception situations are investigated, and that the results of investigations are documented.
21. Determine that files produced from the computer operating system's log monitor are retained long enough to allow investigation of unusual activities.
22. Review procedures for logging problems to determine that all abnormal software and hardware operating conditions are documented.
23. Determine that schedules exist for the submission of critical input batch files and that procedures exist to follow up on missing data.
24. Review procedures to prohibit unauthorized input or access to production files and programs.
25. Review a limited sample of production batch applications to determine that appropriate system control techniques are used.
26. Determine whether users or information systems personnel are responsible for reviewing output controls and assess whether those control reviews are being performed.
27. Assess procedures for reviewing distributed output reports to determine whether they are complete.

detailed review. This would be the same as if internal audit attempted to perform a review of "manufacturing" in a major plant environment. Rather than cover all manufacturing functions, internal audit might review production control one year and receiving and inspection the next, and eventually cover most significant functions. For a specialized review of a specific IT control area, such as memory media library management, internal audit should expand on the procedures developed for a general controls review in that area and add additional audit tests as necessary.

4. **Reviews to assess compliance with laws or regulations.** One of the major objectives of internal control, as discussed in Chapter 3 on internal control fundamentals, is compliance with laws and regulations. Internal auditors should always be aware of objectives in this area and include appropriate tests in their reviews. Auditors working with governmental agencies or in enterprises that do extensive governmental contracting often may be required to perform IT-related compliance audits to determine if appropriate laws and regulations are being followed. These will differ very much from agency to agency and from one political division to another.

Often a compliance-related IT review can be combined with a preliminary or detailed general controls review, but auditors must be aware of the relevant procedures and regulations, such as those published by the governmental agency requiring the audit. Most bank-examination agencies, for example, have published IT controls guidelines. When operating in this type of environment, internal auditors must become aware of the regulatory environment as well as any published procedures.

18.5 ITIL Service Support and Delivery Infrastructure Best Practices

As defined previously, ITIL is the acronym for the information technology infrastructure library, a set of best practices first developed in the 1980s by the British government's Office of Government Commerce (OGC), formerly called the Central Computer and Telecommunications Agency. It is a vendor/supplier independent collection of best practices that has become widely recognized in IT operations, first in the United Kingdom, then in the European Union community (EUC), Canada and Australia, and now increasingly in the United States. ITIL is a detailed framework of significant IT best practices, with comprehensive checklists, tasks, procedures, and responsibilities designed to be tailored to any IT organization. Dividing key processes between those covering IT service delivery and those for service support, ITIL has become the de facto standard for describing many fundamental processes in IT service management, such as configuration or change management.

ITIL is a formal "library" of technical publications, all published by the British OGC.[2] The publications and their contents are tightly controlled, similar to the ISO (International Organization for Standardization) international standards publications discussed in Chapter 30. Internal auditors should be aware of the existence of ITIL and should ask their IT functions how much they have embraced of adopted ITIL best practices. Our intent here is not to provide a detailed description of ITIL's components but to give internal auditors a high-level understanding of some of its components. An understanding of ITIL will allow internal auditors to better understand some key IT processes and to make more effective recommendations when review IT general controls.

ITIL best practices cover what we frequently call the IT infrastructure—the supporting processes that allow IT applications to function and deliver their results to systems users. All too often, internal auditors have focused their attention on the application development side of IT and ignored important supporting service delivery and support IT processes. An enterprise can put massive effort into building and implementing a new budget forecasting system, for example, but that application will be of little value unless there are good processes in place, such as problem and incident management, to allow users of this system to report systems difficulties. Also needed are good capacity and availability processes to allow the new application to run as expected. These ITIL processes are all part of the *IT infrastructure*. A well-designed and controlled application is of little value to its users without strong service support and delivery processes in place. Internal auditors should have a good understanding of these enterprise processes and then develop an appropriate test of controls. These may have been covered in an IT general controls review, and ITIL provides a good general best practices model to follow.

While they have become fairly common throughout the world, ITIL best practices are just now becoming more widely recognized in the United States and have not yet been adequately recognized by internal auditors. The next subsections provide an overview of some ITIL processes that are important for internal auditor IT reviews, including such areas as capacity or service-level management. ITIL best practices should give internal auditors some guidance on how IT functions, such as a help desk, provide areas for internal controls, and recommend controls improvements in this very important IT process area. In most respects, ITIL does not introduce a totally "new" way of building and managing controls but suggests ways to

implement and operate infrastructure general controls that should have already been in place.

ITIL processes traditionally have been split between those covering service support and those for service delivery. Service support processes help make IT application operate in an efficient and customer-satisfying manner, while service delivery processes improve the efficiency and performance of IT infrastructure elements. There are five ITIL service support best practice processes ranging from release management, for placing a process into production, to incident management, for the orderly reporting of IT problems or events. ITIL service support processes cover good practices for any IT enterprise, whether a centralized operation using primarily classic legacy mainframe systems, as its IT central control point, to highly distributed client-server operations. Because of the many variations possible in an IT operations function, ITIL does not prescribe the details of "how" to implement service support processes, such as configuration or change management. Rather, it suggests good practices and ways to manage inputs and relationships between these processes. There is no order or precedence among each. They can be considered and managed separately, but all of them are somewhat linked to one another. Exhibit 18.5 shows a high-level view of the ITIL framework. It shows that the service management areas of service delivery and support, along with security management, provide a linkage between the business operations and IT technology and infrastructure management.

Although there are many separate but interrelated elements to ITIL, this section only discusses ITIL's five defined service support processes, areas that are important for an internal auditor performing an IT general controls review. They suggest preferred approaches for an IT operations function to organize and operate its production systems in a manner that will promote efficient operation and will deliver quality services to the ultimate user or customer of these services. These approaches are particularly useful for an internal auditor performing a review and making recommendations in an IT operations area.

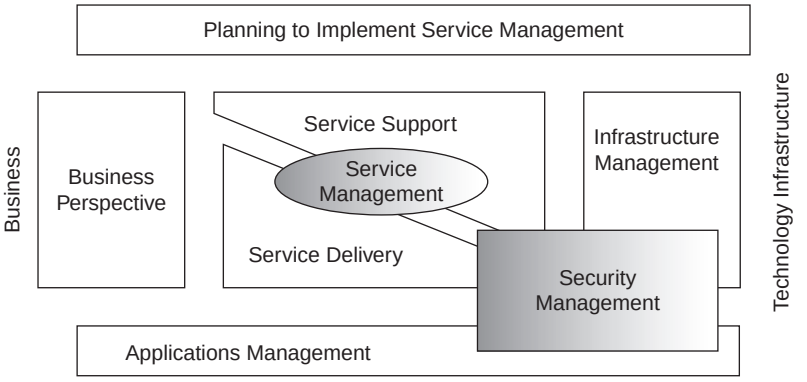


EXHIBIT 18.5 ITIL Framework

Source: Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, COBIT, and ITIL, Robert R. Moeller; Copyright © 2008, John Wiley & Sons. Reprinted with permission of John Wiley & Sons, Inc.

When an internal auditor is observing and reviewing IT operations internal controls, it is useful to think of things in terms of these separate ITIL processes. For example, the ITIL process called incident management, or what has traditionally been called the help desk, is a facility where systems users or their customers can call in to IT operations with a question or problem. While a help desk function can be very useful, it is often a source of grousing when, for example, similar problems are called in repeatedly with no evident efforts to analyze and initiate a solution to the problem. Going beyond just a casual help desk and thinking of this as an overall process where matters are reported to other supporting processes will improve performance and the overall quality of IT operations.

(a) ITIL Service Support Incident Management

Incident management processes cover the activities necessary for restoring an IT service following a disruption. ITIL defines a disruption as any type of problem that prevents an IT user from receiving adequate services, whether an overall system failure, the user's inability to access the application for any of a wide variety of reasons, a password failure due to a "fat fingers" typing error or any other problem. The reported problem is called an *incident,* some type of deviation from standard operations. We use this terminology to refer to incidents throughout our discussion of ITIL. Although many IT have a function called a help desk or a customer support group, we refer to this general function here as the *service desk*. The service desk is usually the owner for the incident management process, although all service support groups across IT may have a role.

The objective of effective incident management processes is to restore normal operations as quickly as possible in a cost-effective manner with minimal impact on the overall business or the user. How quickly is "quickly" should not be subject to interpretation, and ITIL calls for restoration time frame standards to be defined in what are called service-level agreements (SLAs) between IT and the customer or user. Effective SLAs are an important component of the IT infrastructure and are discussed in Section 18.6 as one of the ITIL service delivery processes; their existence should be on internal auditor's radar screens. The first component of the ITIL incident management process is the detection and documentation of the incident by the service desk, as a single point of contact. These incidents can include such matters as a user calling in some specific application problem to IT operations informing the service desk of an application processing problem.

Once the service desk receives an incident, the service desk should classify it in terms of its priority, impact, and urgency. The definition of a reported incident's priority is one of the more important aspects of managing IT incidents. Every person who calls in an incident thinks that his or hers is the most important; the incident management function has the difficult task of defining the relative priority of the reported incident, its importance, and its impact on the business. Exhibit 18.6 shows the life cycle of an incident from the initial call through resolution and closure. Our point here is to help internal audit to understand not how to manage a service desk process but rather its recommended best practices. An understanding of ITIL best practices allows an internal auditor to ask some probing questions when reviewing IT general controls. For example, internal auditors should look for formal SLAs, as part of the service-level management process, to define the priority with which

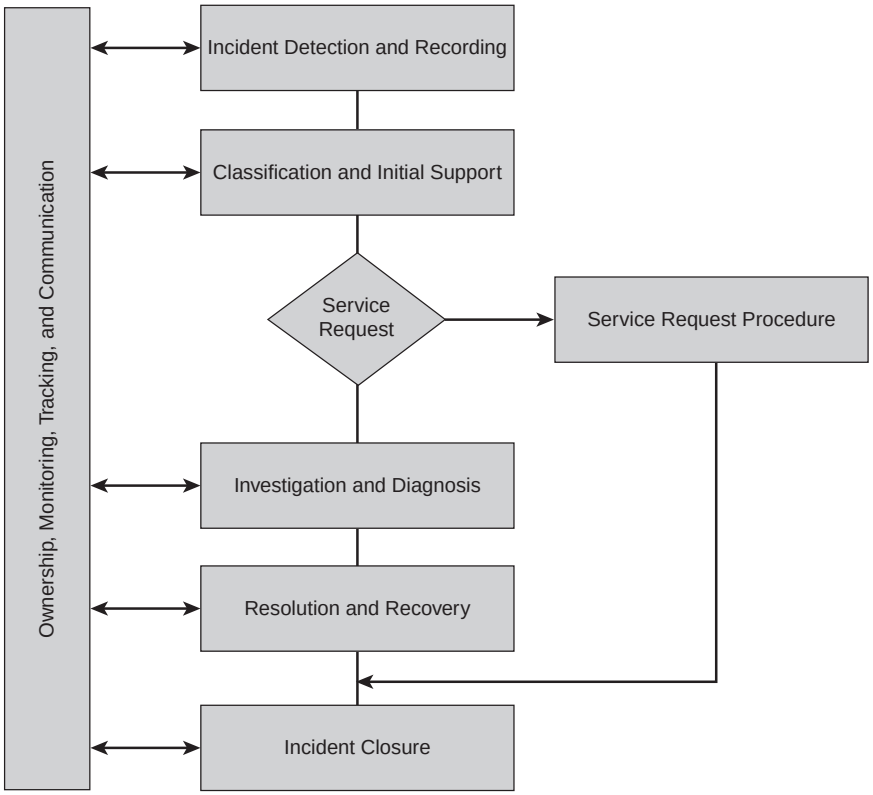


EXHIBIT 18.6 ITIL Incident Management Life Cycle

incidents need to be resolved and the effort put into the resolution of and recovery from incidents. These SLAs should depend on:

- **The *impact or criticality* of the incident on the reporting entity or overall enterprise.** Incident management should assess, for example, how many users will suffer as a result of a reported technical failure of a hardware component. Similarly, a call regarding a problem with the month-end close process should be assigned a higher level of criticality than a problem with the system that generates purchase orders.
- **The *urgency* of the reported incident.** *Urgency* refers to the speed necessary to solve an incident of a certain impact. A high-impact incident does not, by default, always have to be solved immediately. An incident call reporting that some user group cannot work at all because of some service outage is often of greater urgency than a senior manager calling to request a functionality change.
- **The *size, scope, and complexity* of the incident.** The incident management team should investigate the reported incident as soon as possible to determine its extent. A reported failure of some component may just mean that a device is out of service or might indicate a server is down. Often those types of incidents are not that complex and can be repaired relatively easily. A telecommunications failure that might impact multiple international units and thus might delay the monthly financial close can be much larger in size and scope.

Once an incident has been logged in, the process of investigation and diagnosis should begin. If the service desk cannot solve the incident, it should be assigned to other IT support levels for resolution. However, all parties that work on the incident should keep records of their actions by updating a common incident log file.

Some incidents can be resolved through a "quick fix" by the service desk, others by a more formal problem solution. In the case of more significant problems, a work-around to get things back in partial operation may be required coupled with a formal request for change (RFC) to systems, to a vendor, or to whatever parties are need to correct such a problem. In any event, efforts should be marshaled to correct the problem with the incident management function retaining ownership of the matter until resolution. Solid documentation should be maintained to track the incident until its resolution. The incident can be formally closed once matters have been fixed. If not easily solved, the incident should be passed to the ITIL problem management process function.

All ITIL processes are somewhat related to one another, and we have selected incident management as the one to discuss. In many instances, incident management represents the first line between users of IT services and IT itself. Properly organized, incident management should be much more than the help desks of an earlier time when users called in with problems but did not get much help beyond perhaps password resets. Incident management is a first point of contact between the customers—users—and the overall IT function. Incidents, the result of failures or errors within the IT infrastructure, result in actual or potential variations from the planned operation of services. Sometimes the cause of these incidents may be apparent and can be addressed or fixed without the need for further investigation. In other situations, there may be a need for a hardware or software repair, a matter that often takes some time to implement. Short-run solutions may be a work-around, a quick fix to get back in operation, or a formal RFC to the change management process to remove the error. Examples of short-term work-arounds might be instructing a customer to reboot a personal computer or resetting a communications line, without directly addressing the underlying cause of the incident.

Where the underlying cause of the incident is not identifiable, it is often appropriate to raise a problem record for the unknown error within the infrastructure. Normally a problem record is raised only if investigation is warranted, and its actual and potential impact should be assessed. Successful processing of a problem record will result in the identification of the underlying error, and the record can then be converted into a known error once a work-around has been developed and/or an RFC submitted.

(b) Service Support Problem Management

When the incident management process encounters a deviation with an unknown cause or reason, that incident should be passed on to the problem management process for resolution. The objective here is to minimize the total impact of problems through a formal process of detection and repair as well as taking actions to prevent any reoccurrence. The problem management process is an important step in assessing the criticality of some reported incident and should be considered in terms of three problem management subprocesses: problem control, error control, and proactive problem management. ITIL defines a "problem" as an unknown underlying cause resulting from one or more incidents. A "known error" is a problem

that has been diagnosed successfully and for which a work-around has been identified. The idea is not necessarily to create a second administrative function in an IT enterprise to take reported help desk incidents but to identify when and how some help desk–reported incidents should be passed on another person or authority to better diagnose the reported matter and treat it as a problem. An effective problem management process can do much to improve overall IT customer service.

In addition to solving any single incident that was bumped up to the problem management process, IT should try to establish processes for better problem and error control, including maintaining data to help identify trends and suggesting improved procedures for the proactive prevention of problems. Data should be maintained on solutions and/or any available work-arounds for a resolved problem and closed problem records. In many instances, problem management may encounter a situation where it is necessary to go a step further and file a formal RFC, either through IT development function or through a hardware or software vendor.

The problem management process focuses on finding patterns among incidents, problems, and known errors. A detailed review of these patterns allows an analyst to solve the problem by considering the many possibilities and narrowing things down to a solution; this is called root cause analysis. There are many good techniques for resolving and correcting problems, which often are caused by a combination of technical and nontechnical factors. An internal auditor reviewing problem management processes should look for documented formal procedures to support problem analysis and resolution. Problem management is a good area for internal audit to diagnose IT service delivery processes in order to better understand the overall health of IT operations. Areas where internal audit may ask some questions here include:

- The number of RFCs raised and the impact of those RFCs on the availability and reliability of the overall IT services covered
- The amount of time worked on investigations and diagnoses for various types of problems by organization unit or vendor
- The number and impact of incidents occurring before a root problem is solved or a known error is confirmed
- The plans for resolution of open problems with regard to people and other resource requirements as well as related costs and budgeted amounts

The ITIL service support problem management process is an important area for internal auditors to consider and understand when assessing the overall health of IT infrastructure operations. An efficient incident management process is necessary to receive customer calls and take immediate corrective actions, but an effective problem management process will go a step further to analyze and solve the problem, initiating RFCs where necessary and otherwise improving IT customer satisfaction.

(i) **SERVICE SUPPORT CONFIGURATION MANAGEMENT** Whatever their relative size, IT operations functions are complex with multiple types and versions of hardware and software components that must work together in an orderly, well-managed manner. This is certainly true for both a major corporation with classic mainframe systems, "farms" of servers, and a multitude of storage devices and communications gear as well as small IT systems operation. A formal configuration management function is

an important service delivery process that supports the identification, recording, and reporting of IT components, their versions, constituent components and relationships. Items that should be under the control of configuration management include hardware, software, and associated documentation. Configuration management is not the same concept as the depreciation accounting process for asset management, although the two are related. Asset management systems maintain details on IT gear above a certain value, their business unit and their location. Configuration management also maintains relationships between assets, which asset management usually does not. Some enterprises start with asset management and then move on to configuration management.

The basic activity of the configuration management process is to identify the various individual components in IT operations, called configuration items (CIs), and then to identify key supporting data for these CIs including their owners, identifying data and version numbers as well as systems interrelationships. These data should be captured, organized, and recorded in what is often known as a configuration management database (CMDB). The team responsible for configuration management should select and identify these configuration structures for the entire infrastructure's CIs, including establishing relationships between each CI and connected components in the overall IT infrastructure configuration. Going beyond just entry on the CMDB, the process should ensure that only authorized CIs have been accepted and that no CI is added, modified, replaced, or removed without an appropriate change request and an updated specification.

An internal auditor can think of the importance of the configuration management process in terms of desktop applications in the audit department. All internal auditors today probably have laptop computers, but unless each has consistent versions of software, there may be difficulties in these internal auditor systems communicating with one another. This is where configuration management is important. It is even more important when attempting to understand the various versions or even types of software and equipment in a large IT operation.

The configuration management process also includes some control elements. A series of reviews and audits should be implemented to verify the physical existence of CIs and check that they are correctly recorded in the configuration management system. Although we have used the word *audit* here, this is not an internal audit process but an ITIL task of the IT team responsible for the configuration management process. Configuration management should also maintain records for CI status accounting to track the status of a CI as it changes from one state to another (e.g., from under development, to being tested, going live, and then being withdrawn).

The CMDB does not have to be a complex, specialized application. An enterprise can establish a very basic level of CMDB just by using spreadsheets, local databases, or even paper-based systems. In today's large and complex IT infrastructures, however, configuration management requires the use of physical and electronic libraries along with the CMDB to hold definitive copies of software and supporting documentation. The CMDB should to be based on database technology that provides flexible and powerful interrogation facilities. It should include the relationships between all system components, including incidents, problems, known errors, changes, and releases.

The existence and controls supporting a CMDB can be a good point for internal audit to understand the configuration management process and its supporting controls. If the enterprise does not have a good CMDB, internal audit can

EXHIBIT 18.7 ITIL Configuration Management Internal Audit Steps

1. Review and understand existing enterprise configuration management practices as well as their interfaces to the service management processes, procurement, and development.
2. Assess the knowledge and capability of existing IT functions and its staff in terms of controls and processes for configuration, change, and release management processes.
3. Review the extent and complexity of existing configuration data, whether held in hard-copy form, in local spreadsheets, or in configuration management databases (CMDB), and develop an understanding of that database and its retrieval tools.
4. Select a production application and understand its definition on the CMDB in detail, including interfaces to change management, release management, other service management processes, procurement, and development.
5. Using the installed CMDB reporting tool, define the inventory of configuration items (CIs) for one system and physically trace reported CIs to actual configuration components.
6. Determine that processes are in place to link configuration management business processes and procedures with the CMDB tools.
7. Test the CMDB and other support tool(s) to determine that key components, software, and documentation have been implemented and controlled on the CMDB.
8. Review the adequacy of facilities to provide secure storage areas to manage CIs (e.g., cabinets, controlled libraries, and directories).
9. Assess the adequacy of processes to communicate and train staff in the importance and use of configuration management.
10. Review problem management processes to determine the extent and appropriateness of their use of the CMDB for resolving problems.
11. Determine that appropriate access and update controls are in place to prevent unauthorized or inappropriate use of the CMDB.
12. Determine that the CMDB receives adequate backups and that it is part of the continuity plan key resources backup and recovery procedures.

anticipate finding significant internal control problems throughout the IT infrastructure. Exhibit 18.7 outlines audit procedures for reviewing an enterprise's configuration management process.

The Configuration Management process interfaces directly with systems development, testing, change management, and release management to incorporate new and updated product deliverables. Control should be passed from the project or supplier to the service provider at the scheduled time with accurate configuration records. In addition, the CMDB can be used by the service-level management process to hold the details of services and to relate them to the underlying IT components. The CMDB can also be used to store inventory details of CIs, such as supplier, cost, purchase date, and renewal date for a license. An additional bonus is the use of the CMDB to cover the legal aspects associated with the maintenance of licenses and contracts.

(ii) SERVICE SUPPORT CHANGE MANAGEMENT The problem management process often results in the need for IT changes ranging program changes to process revisions to improve service or reduce costs. The goal of ITIL change management is to utilize standardized methods and procedures for the efficient and prompt handling of all

changes, in order to minimize their impact on service quality and the day-to-day operations. ITIL change management processes include:

- IT hardware and system software
- Communications equipment and software
- All applications software
- All documentation and procedures associated with the running, support, and maintenance of live systems

The last point is of particular concern to internal auditors. All too often IT hardware and software is changed with little concern given to changing the supporting documentation. Changes to any IT components, (e.g., applications software, documentation, or procedures) should be subject to a formal change management process.

Internal auditors often encounter IT functions where the change management process is haphazard at best. Examples are changes to applications without thinking through their implications on the overall IT infrastructure, incident management fixes that create other changes, or senior management requests for changes to solve short-term or immediate problems. A formal change management process that reviews and approves any proposed changes will almost always improve IT and enterprise internal control processes. The ITIL change management process should be tightly linked to configuration management to ensure that information regarding the possible implications of a proposed change are made available, and any possible impacts are detected and presented appropriately.

Change management processes should have high visibility and open channels of communication in order to promote smooth transitions when changes take place. To improve this process, many IT functions have instituted a formal change advisory board (CAB), made up of people from both IT and other functions within the enterprise, to review and approve changes. A CAB is a body that exists to approve changes and to assist in the assessment and prioritization of changes. It should be given the responsibility of ensuring that all changes are adequately assessed from both a business and a technical perspective. To achieve this mix, the CAB should consist of a team with a clear understanding of the customer business needs as well as the technical development and support functions. Chaired by a responsible change manager, CAB membership should comprise IT customers, applications developers, various experts/technical consultants as appropriate, and any contractor or third-party representatives if in an outsourcing situation. Although a CAB should meet regularly to review and schedule proposed changes, it should not act as an impediment to IT operations. Its aim is to provide orderly scheduling and introduction of all types of IT infrastructure changes.

Efficient overall service management processes require a capability to change things in an orderly way, without making errors and taking wrong decisions. An effective change management process is indispensable for an effective IT infrastructure. When reviewing IT internal controls, internal auditors should look for an effective change management process that provides:

- Better alignment of IT services to business requirements
- Increased visibility and communication of changes to both business and service support staff

- Improved risk assessments
- A reduced adverse impact of changes on the quality of services
- Better assessments of the cost of proposed changes before they are incurred
- Fewer changes that have to be backed out, along with an increased ability to do this more easily when necessary
- Increased productivity of IT customers—through less disruption and higher-quality services
- A greater ability of IT to absorb a large volume of changes

An effective change management process is an important component of IT infrastructure controls. The process must align tightly with other key processes in the IT infrastructure: change, configuration, capacity, and release management.

(iii) SERVICE SUPPORT RELEASE MANAGEMENT IT functions need effective processes to ensure that changes are introduced to all impacted parties in an orderly and well-controlled manner. Release management covers the introduction of authorized changes to an IT service. A release typically consists of a number of problem fixes and enhancements to the service, including new or changed software and hardware needed to implement the required approved changes.

Releases normally are implemented as full releases, where all of the components being changed are built, tested, distributed, and implemented together. This eliminates the danger that obsolete versions of CIs (see Section 18.5b(i)) will be assumed to be unchanged and used within the release. With a full release, all components supporting some application area or system are released as a single component. With all new and existing components bundled together, any problems are more likely to be detected and rectified before entry into the live environment. The disadvantage is that the amount of time, effort, and computing resources needed to build, test, distribute, and implement the full release will increase.

An alternative approach to release management is a delta or partial release process that includes only those CIs that changed since the last full or delta release. A delta release may be more appropriate when a full release cannot be justified due to such factors as the urgency for needed facilities or the size and related resource requirements of a delta release in comparison with a full release. There is no single correct choice, and a decision to do a delta release should be taken case by case with the CAB making necessary recommendations. Internal auditors should understand the importance of well-ordered release processes and should look for established processes as they perform IT general controls reviews.

The preceding sections have outlined ITIL service support processes at a very high level. When reviewing IT general controls, an internal auditor should think of the importance of processes such as configuration management. An internal auditor does not need to be an expert in these ITIL service support areas but should keep them in mind when reviewing IT general controls. An internal auditor should become sufficiently familiar with these processes to understand controls and procedures supporting IT service support.

18.6 Service Delivery Best Practices

The preceding section has outlined the five ITIL service support best practice processes. In addition, there five additional ITIL service delivery processes. Service

support covers the accurate processing of IT applications and components ranging from receiving a reported incident to defining the problem to introducing the change and then releasing it in to production. The equally important ITIL service delivery processes cover areas more closely aligned with the smooth and efficient operation of the overall IT infrastructure. Some of these, such as the continuity management process, traditionally have been near and dear to the hearts of many internal auditors. Others, such as SLAs that define performance and expectations between IT and its customers, should be familiar to internal auditors who encounter similar arrangements in other areas.

(a) Service Delivery Service-Level Management

Service-level management is the name given to the processes of planning, coordinating, drafting, agreeing, monitoring, and reporting on formal agreements between both IT and the providers and recipients of IT services. SLAs represent a formal agreement between IT and both providers of services to IT and IT end user customers. When the first ITIL service-level best practices materials were published in 1989, an SLA was an interesting but uncommon concept. Today many enterprises have introduced them—although with varying degrees of success—and internal auditors should be familiar with and understand the importance of SLAs when reviewing internal IT infrastructure controls.

As an example of a SLA, when IT contracts with an outside provider, such as for disaster recovery backups, the arrangement will be covered by a formal contract where the disaster recovery provider agrees to provide certain levels of service, following some time-response–based schedule. The governing contract here is a SLA between IT and the provider of continuity services. SLA agreements between IT and their customers are even more important here, from an internal control perspective. We have used the term *customer* here for the older and still-common term of IT users. Many groups in an enterprise use IT's services, and as customers, they have expectations of certain levels of service and responsiveness. These arrangements are defined through a SLA, a written agreement between an IT and its customers that defines the key service targets and responsibilities of both parties. The emphasis should be on agreement, and SLAs should not be used as a way of holding one side or the other to ransom. A true partnership should be developed between the IT provider and the customer for a mutually beneficial agreement; otherwise the SLA could quickly fall into disrepute, and a culture of blame may prevent any true service quality improvements from taking place.

In an SLA, IT promises to deliver services per an agreed-on set of schedules and understands there will be penalties if these agreed service standards are not met. The goal here is to maintain and improve on service quality through a constant cycle of agreeing, monitoring, reporting, and improving the current levels of IT services. SLAs should be strategically focused on the business and maintaining the alignment between the business and IT.

Exhibit 18.8 outlines the contents of a typical SLA. Internal auditors would not find this type of document as part of such formal materials as a home mortgage document. Rather, IT customers negotiate the IT service requirements that they are seeking, such as average response times no more than X hours or financial systems close processing completed by X or other factors. To temper expectations and show what could be available, an IT function usually provides a service offerings catalog. Customer IT services requirements should be negotiated and formal SLAs

EXHIBIT 18.8 Sample IT Service-Level Agreement Contents

There is no one form or format for an SLA. The next list provides contents that should be considered for most SLAs:

Agreement Introduction Pages

- Parties to this agreement
- Title and brief description of the agreement
- Signatories
- Dates: start, end, review
- Scope of the agreement: what is covered and what is excluded
- Responsibilities of both the service provider and the customer
- Description of the services covered

Service Hours

- Hours that each service is normally required (e.g., 24/7, Monday to Friday 08:00–18:00)
- Arrangements for requesting service extensions, including required notice periods (e.g., request must be made to the service desk by 12 noon for an evening extension, by 12 noon on Thursday for a weekend extension)
- Special hours allowances (e.g. public holidays)
- Service calendar

Availability

- Availability targets within agreed hours, normally expressed as percentages. The measurement period and method should be stipulated and may be expressed for the overall service, underpinning services, and critical components, or all three. Since it is difficult to relate to simplistic percentage, availability can be measured in terms of the customer's inability to carry out its business activities.

Reliability

- Usually expressed as the number of service breaks, or the mean time between failures (MTBF) or mean time between system incidents (MTBSI)

Support

- Support hours (where these are not the same as service hours), including arrangements for requesting support extensions
- Required notice periods (e.g., request must be made to the service desk by 12 noon for an evening extension, by 12 noon on Thursday for a weekend extension)
- Special hours allowances (e.g., public holidays)
- Target time to respond to incidents, either physically or by other method (e.g., telephone contact, e-mail)
- Target time to resolve incidents, within each incident priority—target varies depending on incident priorities.

Throughput

- Indication of likely traffic volumes and throughput activity (e.g., the number of transactions to be processed, number of concurrent users, amount of data to be transmitted over the network).

Transaction Response Times

- Target times for average or maximum workstation response times (sometimes expressed as a percentile; e.g., 95% within 2 seconds)

EXHIBIT 18.8 (*Continued*)

Batch Turnaround Times
- Times for delivery of input and the time and place for delivery of output

Changes
- Targets for approving, handling, and implementing RFCs, usually based on the category or urgency/priority of the change.

IT Service Continuity and Security
- Brief mention of IT Service continuity plans and how to invoke them, and coverage of any security issues, particularly any responsibilities of the customer (e.g., backup of free-standing PCs, password changes)
- Details of any diminished or amended service targets should a disaster situation occur (if no separate SLA exists for such a situation)

Charging
- Details of the charging formula and periods (if charges are being made). If the SLA covers an outsourcing relationship, charges should be detailed in an annex as they are often covered by commercial in confidence provisions.

Service Reporting and Reviewing
- The content, frequency, and distribution of service reports, and the frequency of service review meetings

Performance Incentives/Penalties
- Details of any agreement regarding financial incentives or penalties based on performance against service levels. These are more likely to be included if the services are being provided by a third-party organization. Note that penalty clauses can create their own difficulties.

established. Performance against these SLAs should be monitored on an ongoing basis with their results reported regularly. Failure to meet these SLA standards could result in additional negotiations and SLA adjustments. This SLA process provides benefits for the business and IT, including:

- Because IT should be working to meet negotiated standards, IT services will tend to be of a higher quality, causing fewer interruptions. The productivity of the IT customers should improve as well.
- IT staff resources will tend to be used more efficiently when IT provides services that better meet the expectations of its customers.
- By using SLAs, the services provided can be measured and the perception of IT operations will generally improve.
- Services provided by the third parties are more manageable with the underpinning contracts in place, and the possibility of negative influence on the IT service provided is reduced.
- Monitoring overall IT services under SLAs makes it possible to identify weak spots that can be improved.

The SLA process is an important component of IT operations. If an enterprise does not use formal SLAs, internal auditors reviewing IT operations general controls should consider recommending implementing formal SLA processes. SLAs can create

a totally new environment within IT, where all parties will better understand their responsibilities and service obligations, with the SLA serving as a basis for resolving many issues. Internal audit can use the SLA as a basis for assessing internal controls in a variety of areas and for making strong controls improvement recommendations.

(b) Service Delivery Financial Management for IT Services

In its earlier days, the IT function in most enterprises was operated as a "free" support service. Its expenses were handled through central management with its cost allocated to benefiting users. There was little attention given to costs in those early days. If a department wanted some new application, they would pressure management to purchase the package and add any additional necessary people to manage it. Over time, IT enterprises began to establish charge-back processes, but these were too often viewed as a series of "funny-money" transactions where no one paid too much attention to the actual costs and pricing of IT services.

Today, the costs and pricing of IT services are or should be a much more important consideration. The well-managed IT function should operate more as a business, and financial management is an important and key ITIL process to help manage the financial controls for that business. The objective of the service delivery financial management process is to suggest guidance the cost-effective stewardship of the assets and resources used in providing IT services. IT should be able to account fully for its spending on IT services and to attribute these costs of services delivered to the enterprise's customers. Three separate subprocesses are associated with ITIL financial management:

1. **IT budgeting** is the process of predicting and controlling the spending of money for IT resources. Budgeting consists of a periodic, usually annual, negotiation cycle to set overall budgets along with the ongoing day-to-day monitoring of current budgets. Budgeting ensures that there has been planning and funding for appropriate IT services and that IT operates within this budget during the period. Other business functions will have periodic negotiations with IT to establish expenditure plans and agreed investment programs; these ultimately set the budgets for IT.
2. **IT accounting** is the set of IT processes for determining how money is spent by customers, services, and activities. IT functions often do not always do a good job in this area. They have a wide variety of external costs, including software, equipment lease agreements, telecommunications costs, and others, but these costs often are not well managed or reported. They have enough data to pay the bills and evaluate some specific area costs, but IT functions often lack the level of detailed accounting found in a large manufacturing enterprise, as an example. A manufacturing cost accounting or activity-based accounting model has applicability for IT accounting best practices.
3. **Charging** is the set of pricing and billing processes to charge customers for the services supplied. This requires sound IT accounting and needs to be done in a simple, fair, and well-controlled manner. The IT charging process sometimes breaks down in an IT function because the billing reports of IT services are too complex or technical for many customers to understand. IT needs to produce clear, understandable reports of the IT services used such that customers can verify details, understand enough to ask questions regarding service, and negotiate adjustments if necessary.

Financial management for IT services provides important information to the service-level management process about the IT costing, pricing, and charging strategies. While generally not operated as a profit center, the financial management process allows both IT and its customers to think of IT service operations in business terms. The financial management process may allow IT and overall management to make decisions about what, if any, functions should be retained in-house or outsourced to an external provider.

The financial management process allows accurate cost-benefit analyses of the IT services provided and allows the IT enterprise to set and meet financial targets. It also provides timely reporting to the service-level management process, such that customers can understand the charging and pricing methods used. Of all of the ITIL service support and delivery processes, financial management is one ITIL best practice that frequently gets short shrift. IT people have a technical orientation and tend to think of financial management as an *accounting issue,* almost beneath them. On the other side of the coin, finance and accounting professionals tend to look at these issues as too technical and beyond such transactions as equipment lease accounting or facility space charges. Internal auditors should use their financial skills as well as IT knowledge to review and assess financial management process internal controls. Exhibit 18.9 provides procedures for an internal audit review of the costs and pricing of IT processes. This is not a common review area for internal audit, but given the large costs distributed to customers as well as the importance of an enterprise's IT resources, it can be an important audit area.

(c) Service Delivery Capacity Management

ITIL capacity management ensures that the capacity of the IT infrastructure is aligned with business needs to maintain the required level of service delivery at an

EXHIBIT 18.9 Costs and Pricing Internal Audit Review Steps

1. Develop and document a general understanding of the cost structure for IT operations, including costs of equipment supplies and salaries.
2. Review and understand costing philosophy for IT operations: Is it an overhead function, cost recovery, or revenue generating?
3. Review processes for costing and pricing IT services:
   a. Are all IT costs covered?
   b. Based on interviews with IT users, does the costing and pricing system appear to be understandable?
   c. Is there a process in place to administer the costing process and to make adjustments if necessary?
4. Review the negotiation process with IT users to understand pricing process: Are expected costs included in SLAs?
5. Select pricing reports during a period for several processes, and check to determine the prices are included in SLAs.
6. Review appropriateness of adjustment process of over a period to determine the corrections are investigated and applied when appropriate.
7. Review data processing services billed for one accounting period and determine whether they cover all actual IT costs. Investigate and report on any differences.
8. For a selected accounting period, trace IT pricing charges to appropriate accounting system entries.

acceptable cost through appropriate levels of capacity. Through gathering business and technical capacity data, this process should result in a capacity plan to deliver cost-justified capacity requirements for the enterprise. Besides its prime objective of understanding an enterprise's IT capacity requirements and delivering against them, capacity management is responsible for assessing the potential advantages new technologies could have for the enterprise.

The capacity management process generally is considered in terms of three subprocesses covering business, service, and resource capacity management. Business capacity management is a long-term process to ensure that the future business requirements are taken into consideration and then planned and implemented as necessary. Service capacity management is responsible for ensuring that the performance of all current IT services fall within the parameters defined in existing SLAs. Resource capacity management has a more technical focus; it is responsible for the management of the individual components within the IT infrastructure. The multiple inputs to these three capacity management subprocesses include:

- SLAs and SLA breaches
- Business plans and strategies
- Operational schedules and schedule changes
- Application development issues
- Technology constraints and acquisitions
- Incidents and problems
- Budgets and financial plans

As a result of these multiple inputs, the capacity management process—often under a single designated capacity manager—will manage IT processes, develop and maintain a formal capacity plan, and make certain capacity records are up to date. In addition, the capacity manager must be involved in evaluating all changes to establish the effect on capacity and performance. This capacity evaluation should happen both when changes are proposed and after they are implemented. Capacity management must pay particular attention to the cumulative effect of changes over a period of time that may cause degraded response times, file storage problems, and excess demand for processing capacity. Other capacity management process responsibilities include some duties of the network, application, and system managers. They are responsible for translating the business requirements into the required capacity to be able to meet these requirements and to optimize IT performance.

The implementation of an effective capacity management process offers IT the benefits of an actual overview of the current capacity in place and the ability to plan capacity in advance. Effective capacity management should be able to estimate the impact of new applications or modifications as well as provide cost savings that are in tune with the requirements of the business. Proper capacity planning can significantly reduce the overall cost of ownership of an IT system. Although formal capacity planning takes time, internal and external staff resources, and software and hardware tools, the potential losses incurred without capacity planning can be significant. Lost productivity of end users in critical business functions, overpaying for network equipment or services, and the costs of upgrading systems already in production can more than justify the cost of capacity planning. This is an important ITIL process, and internal auditors should consider capacity management when reviewing IT infrastructure controls and processes.

(d) Service Delivery Availability Management

Enterprises are increasingly dependent on their IT services on an availability of 7 days per week and 24 hours a day (24/7). When IT services are unavailable, in many cases the business stops as well. It is therefore vital that an IT function manage and control the availability of its services. This can be accomplished by defining the business requirements regarding IT service availability and then matching them with the possibilities of the IT enterprise.

Availability management depends on multiple inputs: requirements regarding the availability of the business; information on reliability, maintainability, recoverability, and serviceability of the CIs; and information from the other processes, incidents, problems, and achieved service levels. The outputs of the availability management process are:

- Recommendations regarding the IT infrastructure to ensure its resilience
- Reports about the availability of IT services
- Procedures to ensure the availability and recovery for every new or improved IT service
- Plans to improve the availability of the IT services

Availability management activities can be described as planning, improving, and measuring actions. Planning involves determining the availability requirements to find out if and how IT can meet them. The service-level management process maintains contact with the business and will be able to provide the availability expectations to availability management. The business may have unrealistic expectations with respect to availability and may not fully understand what it means in real terms. For example, business users may want 99.9% availability yet will not realize that this will cost five times more than providing 98% availability. It is the responsibility of service-level management to highlight and to manage such potential costly expectations.

An IT function can either design for availability or recovery. When the business cannot afford a particular service downtime for any length of time, IT will need to build resilience into the infrastructure and ensure that preventive maintenance can be performed to keep services in operation. In many cases, building extra availability into the infrastructure is an expensive task that can be justified by business needs. Designing for availability is a proactive approach to avoiding downtime in IT services.

When the business can tolerate some downtime of services or when a cost justification cannot be made for building in additional resilience into the infrastructure, designing for recovery is the appropriate approach. Here, the infrastructure is designed such that in the event of a service failure, recovery will be "as fast as possible." Designing for recovery is a more reactive management approach for availability. In any event, processes such as incident management need to be in place to recover as soon as possible in case of a service interruption.

The main benefit of availability management is a structured process to deliver IT services according the agreed requirements of the customers. This should result in a higher availability of the IT services and increased customer satisfaction. Internal auditors often can ask some hard questions as part of their IT general controls reviews in this area.

(e) Service Delivery Continuity Management

As businesses become ever more dependent on IT, the impact of any unavailability of IT services has drastically increased. Every time the availability or performance of a service is reduced, IT customers cannot continue with their normal work. This trend toward a high dependency on IT support and services will continue and increasingly influence direct customers, managers, and decision makers. ITIL continuity management emphasizes that the impact of a total or even partial loss of the IT services should be estimated and continuity plans established to ensure that the business, and its supporting IT infrastructure, will always be able to continue.

ITIL calls for an appropriate strategies that contain an optimal balance of risk reduction and recovery options. Some of these ITIL strategies are discussed in Chapter 22. Using the approaches outlined there, an IT enterprise can implement an effective set of service continuity processes. Internal auditors should refer to the Chapter 22 discussion to better understand and evaluate continuity and disaster recovery planning processes.

18.7 Auditing IT Infrastructure Management

The ITIL service support and service delivery processes introduce an expanded and improved approach for looking all aspects of the IT infrastructure. These processes are not independent and freestanding. While each process can operate by itself somewhat, they all depend on the input and support form other related processes. We have tried to show these interdependencies in several of the process descriptions, and an internal auditor reviewing controls over any of the ITIL processes, must think of these controls in relation to other processes. For example, Exhibit 18.10 shows how ITIL change management processes are dependent on and support other ITIL-related processes.

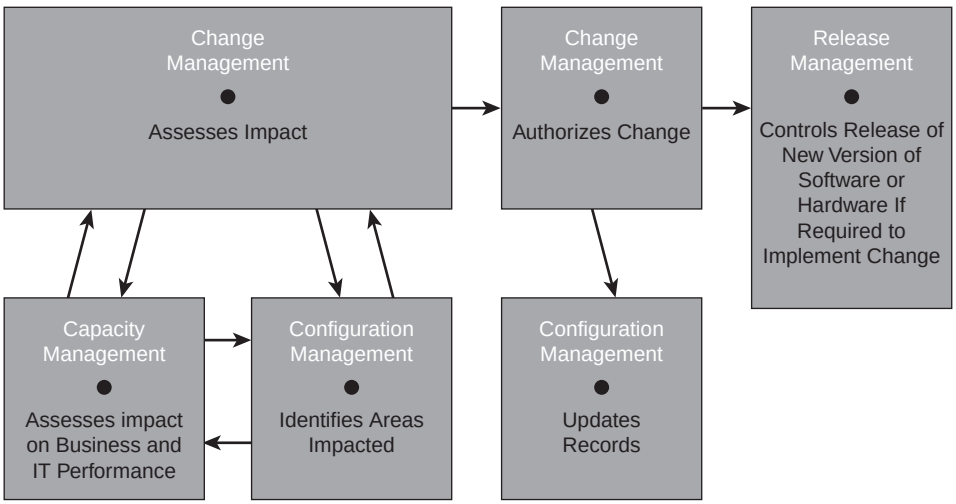


EXHIBIT 18.10 Relationship of ITIL Change Management to Other ITIL Processes

ITIL service delivery and service support are two interrelated and almost parallel elements. They support the management of the IT infrastructure and of the enterprises. IT applications are in the center of this puzzle and are a key central area of internal controls concerns. Our discussions of problem, incident, and change management ITIL processes, among others, tend to call for a very large IT function with multiple levels of staff and management resources. An internal auditor might ask if these ITIL standards apply to an enterprise that is much smaller. Our answer here is very much of a yes, ITIL applies to all sizes of IT functions. In order to be ITIL-compliant, an enterprise does not need multiples levels of support staff. Rather, it needs to think of the various service support and service delivery processes from an ITIL best practices perspective. A small IT function may not need to establish separate incident management and problem management functions but must think of each as separate processes with its unique controls procedures. Even if a very small IT function, each ITIL process area should be treated as important areas for process improvement.

Internal auditors should pay particular attention to ITIL compliance when making recommendations. The size and scope of the area being audited and the scope of operations should always be considered.

The IT infrastructure is an important area for internal audit reviews. In the past, all too often internal auditors concentrated on the applications controls and the IT general controls. The ITIL processes outlined in this chapter are some excellent areas for internal audit attention in today's world of complex processes supporting the IT infrastructure. When reviewing internal controls for any IT enterprise, whether a major corporate-level IT operation or the smaller function found in many of today's enterprises, the effective internal auditor should concentrate on reviewing controls over key IT infrastructure processes.

18.8 Internal Auditor CBOK Needs for IT General Controls

The need for an internal auditor CBOK is an ongoing theme throughout these chapters. In some instances, such as understanding the *International Standards for the Professional Practice of Internal Auditing,* as discussed in Chapter 8, this knowledge should be an essential internal auditor CBOK requirement. In other topic areas, such as Chapter 30's discussion of ISO 9000 and other quality system standards, internal auditors should have a CBOK basic understanding of the area but do not necessarily need a detailed level of knowledge. This chapter has discussed internal audit reviews of IT general controls and the IT infrastructure. These areas represent a strong CBOK requirement for all internal auditors.

As discussed, the world of IT general controls is seemingly constantly changing and evolving. Many technical issues may be best reserved for the IT audit specialists, but all internal auditors should have a strong level of knowledge of IT general controls and the supporting infrastructures that allows those general controls to operate and function.

An internal audit understanding of IT general controls is essential. No matter what size or scope of IT operations, certain controls procedures—such as program revision controls—apply to all operations. In addition, an overall understanding of ITIL best practices should allow internal auditors to understand and evaluate IT

general controls in many environments. The next chapters discuss other IT-related issues that are important to internal auditors, such as cybersecurity and continuity planning

Notes

1. A hash total is a summation of the numeric and alphabetic values for some computer value. It is used as a control total.
2. ITIL publications are available from the U.K. agency called The Stationery Office and can be found through www.tsoshop.co.uk.

CHAPTER 19

Reviewing and Assessing IT Application Controls

Information technology (IT) applications drive many if not most of today's enterprise processes. These IT applications range from the relatively simple, such as an accounts payable system to pay vendor invoices, to the highly complex, such as an enterprise resource management (ERM) set of interrelated database applications to control virtually all enterprise processes. Many IT applications are based on vendor-purchased software; an increasing number come from Web-based services; some are developed by in-house development teams; and many others may be based on spreadsheet or database desktop applications. While the IT general control procedures discussed in Chapter 18 cover best practices over all IT operations, specific control processes should also be associated with each installed IT application. In order to perform internal controls reviews in specific areas such as accounting, distribution, or engineering, internal auditors must have the skills to understand, evaluate, and test the controls over the supporting IT applications. Reviews of specific application controls often can be more critical to achieving overall audit objectives than reviews of general IT controls.

Application controls, however, are very dependent on the status of overall IT general controls discussed in Chapter 18. For example, if there are inadequate controls over an IT systems configuration management process, it will be very difficult for an internal auditor to rely on the controls built into a specific application. Even though internal audit may find that an order-entry application is properly screening sales orders for valid credit approvals, the surrounding general controls covering change configuration management must also be considered. Without IT configuration management update controls, for example, the order-entry system's programs could be changed, without management's authorization, perhaps to override established credit approval controls.

A typical enterprise may have a large and diverse number of production IT applications. They will support a wide variety of functions within the enterprise, starting with accounting but including such areas as manufacturing, marketing, engineering, and others. These supporting application systems are implemented using a variety of IT technologies, such as centralized systems with telecommunication networks, Internet-based systems, client-server applications, and even older mainframe batch-processing systems. Some of these applications may have been developed in-house, but increasingly large numbers of them are based on purchased software packages installed locally or accessed through Web-based service providers.

In-house-developed applications may be written in a language such as C# (also called C-sharp) or Visual Basic, a database report-generator language such as SQL, or the object-oriented language Java. Applications documentation may range from very complete to almost nonexistent. Despite the best efforts of internal audit to suggest improvements, the same can often be said about application controls.

While members of management may not have a good understanding of some IT general controls issues, typically they are interested in internal audit findings covering specific application controls reviews. For example, while an audit finding on general controls over computer operating systems program libraries may not generate management interest, a finding of an incorrect discount calculation based on a foreign currency conversion problem in an accounts payable application is sure to draw attention. However, because of the relative complexity of many IT applications when their controls reside both within the application and in supporting user areas, audits of many IT applications can be a challenge to the modern internal auditor.

This chapter discusses how internal auditors can effectively review internal accounting controls in IT applications, including assessing risks in selecting applications for review, developing an understanding of application controls as well as evaluating and testing those controls, and reviewing new applications under development. We focus on the internal control characteristics of different types of applications and then how to select appropriate applications in internal controls reviews. While there are many differences from one application to another, this chapter focuses on how an internal auditor should select higher-risk applications as candidates for internal audit reviews, the tools and skills needed to understand and document application internal controls, and finally, processes to test and evaluate those applications. Today, all internal auditors should have an understanding of evaluating and assessing IT applications internal controls as part of their basic common body of knowledge (CBOK) skills.

19.1 IT Application Control Components

An internal auditor should understand the elements of a typical IT application and their need for supporting controls. People not familiar with IT sometimes think of an IT application just in terms of the system output reports or the data displayed on terminal screens. However, every application, whether Web-based, an older mainframe system, a client-server application, or an office productivity package installed on a local desktop system, has three basic components: (1) system inputs, (2) programs used for processing, and (3) system outputs. Each of these has an important role in an application's internal control structure.

Early IT applications could be separated into these three components easily. The traditional computerized payroll system from long ago used time cards and a personnel paymaster file as its inputs and a set of programs to calculate pay and benefits as well as to update pay history records. The outputs from that payroll system were the printed checks, payroll register reports, and updated paymaster files. Today, that same payroll system might accept inputs from an automated plant badge reader that controls accesses and tracks attendance, a shop-floor production system that performs incentive pay calculations, various other online inputs, and a human resources database. A series of computer programs, some located at a Web-based service provider and others distributed to remote workstations, would

do the processing. In many cases today, much of the payroll processing is handled by an outside service function that does most of these activities. The modern payroll system's outputs include transactions to transmit compensation to employee bank accounts, pay vouchers mailed to employees, input files to various tax and benefit sources, various display screens, and an updated human resources database.

While the input, output, and computer processing system components may not be all that clear to an internal auditor performing an initial review, the same three elements exist for all applications. No matter how complex the application may appear to be, an internal auditor should always develop an understanding of an application by breaking down its input, output, and processing components. The next sections briefly discuss some of the control aspects of these application components to give an overview on modern IT applications. All internal auditors should have, at the very least, a general understanding of IT applications and supporting processes—a basic CBOK requirement.

(a) Application Input Components

Every IT application needs some form of input, whether data are manually input from transaction vouchers or supplied from some other automated system. Think of a common handheld calculator: The device will generate no results unless data of some sort are input through the key panel. Although the computer programs in an application process the data, determine the outputs, and have a major impact on controls, an internal auditor should always understand the nature and sources of the input components. In traditional, batch-oriented systems, this was a fairly easy process; inputs often were sequential records recorded on a magnetic tape file or even as 80-column punched cards. Today, inputs often are generated from various automated sources, including wireless data collection devices and specialized bar code readers.

(i) DATA COLLECTION AND OTHER INPUT DEVICES As mentioned, very early IT applications used punched cards as their input source. A single card carried 80 or 90 columns of alphanumeric encoded data, and users entered their transactions on data collection sheets for keypunching onto these card formats. The original data collection sheet was the first step in the input chain, and internal auditors were concerned that all transactions were keypunched correctly. These cards were then machine-sorted or otherwise manipulated prior to entry into a system, either read directly into a computer program or copied to magnetic tape for subsequent processing on a batch basis. That is, 500 lines of transactions may have been prepared on data collection sheets and processed as a batch. The need for all transactions to be keypunched correctly and subsequently read into the computer program made input transactions controls a key component of an application's overall internal controls.

Technological improvements have eliminated those punched cards and keypunched input records. Batch-type transactions that must be entered into a computer application are no longer entered by a specialized "keypunch" or data entry department. Rather, operational departments use online terminals to enter their transactions for collection and subsequent processing. Following a processing schedule, these transactions may be applied upon input or collected and updated later in a batch mode. The data entry programs used to capture them often have some transaction-screening capabilities to eliminate any low-level errors common to earlier batch

input systems. In many other situations, the entry of a transaction updates files in a real-time mode.

Transaction input data comes from many sources. A retail store captures sales inputs through a combination of sales entries entered on the point-of-sale (POS) terminal and product sales are entered through bar code readers. Similarly, data are captured on a manufacturing shop floor through various tickets and badges that are entered in readers by workers directly on the shop floor. A small computer chip, called a radio-frequency ID (RFID), embedded on the label of the component may provide inputs as to the product's identification and any subsequent movements. These are all input devices generating transactions for updating to some type of processing application. Input transactions are increasingly generated not from within the enterprise but from applications located in other physical locations and controlled by others. Enterprises today receive a wide variety of data transactions through the Internet or electronic data interchange (EDI) systems, or wireless systems. Here, another enterprise may submit purchase order transactions, accounts payable remittances, or other significant business transactions. Individuals initiate sales transactions, trade securities, and perform other business through their home computers via the Internet. All of these represent input transactions to various IT applications, and each has its own unique control considerations.

An internal auditor reviewing input controls over IT applications should always look for some of the same basic internal control elements found in all enterprise processes. For example, there should be some means of checking that only correct data are entered. A computer program that, through its supporting validation tables, can verify that a part or employee number is or is not valid cannot easily verify that the current quantity should have been entered as 100 as opposed to 10. The older batch systems had hash total checks to help check for these possible errors. A hash total is a nonmonetary value, such as the "sum" of all account numbers. Modern systems need reasonableness checks built into their data-collection procedures, and the programs processing the transactions need controls to prevent errors or to provide warning signals.

(ii) APPLICATION INPUTS FROM OTHER AUTOMATED SYSTEMS Computer applications are often highly integrated, with one application generating an output file of data for processing by another. The transaction entered into one application may impact a variety of other interrelated applications. Thus, an error or omission of an input at one point in a chain of applications may impact the processing of another connected application. In addition to understanding the sources of the transactions to an application, an internal auditor should understand the nature of other automated inputs to that same application. For example, a modern payroll system may receive inputs from a sales performance system to calculate commissions. The sales performance file that feeds the payroll system is another input. The controls there are based on the input, processing, and output controls of the sales performance system. If sales performance data represent a significant input to the payroll system, an internal auditor needs to be concerned about the controls over it as well as over any other supporting applications.

A large network of interconnected applications can present a challenge to an internal auditor attempting to review the input controls for just one interconnected application. For example, an internal auditor may be interested in understanding application input controls for application X. However, files from related applications

A, B, and C may provide inputs to X while D and E provide inputs to applications A and C, respectively. In order to review input controls, an internal auditor typically does not have the time or resources to review all of these processes. Rather, he or she must decide on the most critical of them and assume the other less critical supporting applications are generating appropriate transactions.

(iii) FILES AND DATABASES Although generated by either some other supporting application or updated by the application under review itself, an application's files and databases represent important inputs. In some instances, these files represent tables of data used for the validation of program data. As part of gaining an understanding of an application, the internal auditor should understand the nature and content of all supporting application files. The software that controls these files generally has various record-counting and other logical controls to determine that all transactions are correctly written onto and can be retrieved from the supporting electronic media. Files also have their own dating and label-checking controls to prevent them from being input improperly to a wrong processing cycle or an incorrect application. Once written as streams of sequential records on magnetic tape, today's files are input onto higher-density tape cartridges or magnetic disc memory cards. The internal auditor needs a general understanding not only of the type and nature of inputs to a computer application but also of the source of the file data and any controls over it, as will be discussed in greater detail in Section 19.4.

Databases can represent a particular challenge to an internal auditor. Although the term *database* is often misused to refer to almost any type of computer file, an IT database is a file that organizes data in a format such that all important data elements point or relate to each other. In past years, many mainframe computers used what were called *hierarchical databases,* where data was organized in a grandfather-father-son "family tree" type of structure. An older IBM mainframe product called IMS (Integrated Management System) was once a popular type of a hierarchical database. Using it in a manufacturing enterprise, each product might be organized as a header record that would point to each of its parts. Those components, in turn, would each have a hierarchy of records comprising its individual parts. File integrity was very important here because a program error that breaks one of the connecting chains would make it difficult to retrieve the lost data.

Today, the relational database is a much more common file structure and is found on all types and sizes of computers. A relational database is like a multi-dimensional Excel spreadsheet. That is, the user can retrieve data across various database rows, columns, and pages rather than having to go to the head of each tree and then search down through that tree to retrieve the desired data. Besides being a very effective way to organize input data to application systems, these databases allow for easy retrieval of end user–oriented reports. Two common examples of this very efficient relational database model are Oracle Corporation's database products and IBM's DB2 database.

(b) Application Programs

Applications are processed through a series of computer programs or sets of machine instructions. A traditional payroll system, for example, would consist of a series of computer programs: One would read the employee's time card data, store the number of hours worked, and then use the employee number on that input time

card to look up the employee's rate and scheduled deductions. Based on this match, the program looks up the employee's rate of pay and multiplies this by the number of hours worked to calculate the gross pay.

A computer program is a set of instructions covering every detail of a process. Writing a program is the process of writing detailed instructions and then following them to the letter. As an experiment to comprehend the details required writing a larger computer program, an internal auditor should try to write down each step to follow in the morning from the time the alarm goes off until arrival at the office. Do this one day, documenting all typical actions as well as alternate decision paths, such as whether to dress normally for work or for "casual" Friday. The following morning, use these same instructions *exactly* as they are written to get up, wash, dress, and then go off to work. Most will arrive at work missing an item of clothes or worse. This is the difficulty of writing detailed computer programs. It is usually not necessary for internal auditors to know how to write formal computer programs beyond the simple audit-retrieval applications discussed in Chapter 21, but effective internal auditors should understand how computer application programs are built and what their capabilities are, in order to define appropriate control procedures.

(i) TRADITIONAL MAINFRAME AND CLIENT-SERVER PROGRAMS Mainframe, or what we often call legacy-type computers, were used extensively for business applications beginning in the early 1960s. Although these applications were first programmed in early computer languages on what are now called first-generation actual machine languages based on binary 1s and 0s, we quickly moved to the second generation of what are called assembly languages. These symbolic languages used codes to represent instructions such as to add or store a value. Third-generation languages soon followed. They used actual English-like instruction statements, such as "`ADD A TO B`," to describe the actions to be taken. Programs called *compilers* translated these instructions into machine language. Although many of these compiler languages were introduced in the 1960s, COBOL[1] became the almost standard language for business data processing well into the 1980s. Illustrating its English-like character, Exhibit 19.1 shows an example of the COBOL programming language. It is still in use today for many business applications; however, specialized database and report-generator languages as well as object-oriented languages are making increasing inroads.

The manner in which COBOL business programs are written has changed over the years as well. Earlier programs followed almost no standards. A programmer might insert a variable value, such as an overhead rate, into the COBOL code. When that rate changed at a later date, a programmer had to search through the program listing because often the language provided insufficient index cross-references. Early programs were sometimes written with program logic that was difficult to follow and in which control errors were possible. These COBOL program "sins" were a major reason for many of the worldwide corrective action efforts as we moved from the 1990s to the year 2000. Older computer programs had defined key processing calendar computer dates in a COBOL "mmddyy" format. Because of a lack of supporting documentation, there was a concern that many programs would fail as we went from a date yy value of 99 to 00.

There was a massive effort to remedy this Year 2000 or Y2K problem.[2] This author, for example, was involved in projects ranging from fixed asset financial

EXHIBIT 19.1 COBOL Programming Language Example

1. COBOL is an English-like language that uses verbs to describe the actions to be performed and alphanumeric symbols to describe data fields. For example, employee hours worked might be described as a program file data item called HOURS-WORKED, and the pay rates for employees might be called just that, PAY-RATES. These pay rates would be carried in a program table for all employees, and the COBOL program language instruction for the employee pay calculation would be organized in a paragraph of instructions called PAY-CALC:

   ```
   MULTIPLE HOURS-WORKED BY PAY-RATES GIVING GROSS PAY ROUNDED
   ```

   This program language statement calculates a rounded value for GROSS-PAY that is then used for further payroll processing.
2. COBOL program statements are organized as a test where sets of instructions are grouped by paragraphs. The set of instructions for the pay calculation might be called a GO TO instruction. The very last lines of the above pay calculation might be:

   ```
   PRINT FINAL-PAY
   GO TO PAY-CALC
   ```

   These final two instructions would complete the pay calculation for one employee and then go back to the beginning of the list of employees for the next employee.
3. COBOL programming is based on sets of logical rules covering each item process. While the language can be easy to learn, COBOL programs can also be very complex and difficult to read and understand.

applications to process food manufacturing. Although much effort was expended worldwide, applications were corrected and IT applications generally recovered. From an internal audit and internal control perspective, this is an example of the need for strong documentation and internal controls in all IT applications.

A wide range of computer languages are used today. In addition, many applications are developed through English language–like report-generator languages that reside on top of a supporting computer language. Other than being able to write an audit retrieval request, as discussed in Chapter 21, today's internal auditor does not need to have skills in a programming language.

(ii) MODERN COMPUTER PROGRAM ARCHITECTURES In the days of mainframe computers, business applications developed in-house were almost always written in COBOL. Today, most enterprises generally purchase or lease their packages or access them through a Web service provider, but some IT functions still develop their own applications in-house, using a wide variety of programming tools beyond the traditional COBOL, such as what are called object-oriented programming languages. In-house development normally occurs when an enterprise has business requirements where no commercial software packages seem precisely correct, or more significantly, when an enterprise has plans for some strategic software-based initiative. Today's internal auditor, even one with a fundamental knowledge of Visual Basic, COBOL, or C, may have some difficulties understanding how these object-oriented applications are programmed and constructed. Often they consist of many

EXHIBIT 19.2 Object-Oriented Programming Language Concepts

Object-oriented programming (OOP) programming languages, such as Java and C++, are organized around "objects" of data rather than logic-based "actions." Programs using languages, such as COBOL, were based on logical procedures that took input data, processed it, and produced output data. These older programming approaches described the processing logic but did not define the data. Object-oriented programming focuses on the data objects we want to manipulate rather than the logic required to manipulate them. Examples of objects range from human beings (described by name, address, etc.) to buildings and floors (whose properties can be described and managed) or the little individual parts in a manufactured produce.

The first step in OOP is to go through a data modeling exercise and identify all the objects you want to manipulate and how they relate to each other. Think of all of the furniture in the board of director's meeting room. There will be a major table for board meetings and side tables for the supporting staff. The chairs in that room will be *Object*s with each director, around the table, having one *Class* of chair, the support staff another class, and the CEO at the end of the table with still another. These *Objects* are then generalized into *Classes of Objects*. OOP defines the logical sequences of these classes of objects. The director's chairs are arranged around the board conference table, the CEO at the end, and support staff off to the sides. OOP provides computer instructions, based on the relevant data in the class object characteristics, to allow the objects and their characteristics to communicate with each other in well-defined interfaces called *Messages*. For example, the CEO's chair will be at the head of the table, and if the CEO is present, messages will be delivered to other board members.

The concepts and rules used in object-oriented programming provide these important benefits:

- The concept of a data class makes it possible to define subclasses of data objects that share some or all of the main class characteristics. Called *inheritance*, this property of OOP forces a more thorough data analysis, reduces development time, and ensures more accurate coding.
- Since a class defines only the data it needs to be concerned with, when an instance of that class (an object) is run, the OOP program will not be able to access other program data accidentally. This characteristic of *data hiding* provides greater system security and avoids unintended data corruption.
- The definition of a class is reusable both by the program for which it is initially created and also by other object-oriented programs. (For this reason, a class can be more easily distributed for use in networks.)
- The concept of data classes allows a programmer to create new *data types* that are not already defined in the language itself.

The OOP languages C++ and Java are the most popular object-oriented languages today, with Java designed especially for use in distributed applications on corporate networks and the Internet.

very small program code modules that pass data to one another, sometimes over remote telecommunication lines. While it is certainly not an internal audit CBOK need, Exhibit 19.2 describes some high-level concepts of object-oriented programming. These programming languages, such as Java and C++, are the languages of today's Web-based applications.[3] An internal auditor should rely on the overall application program standards in place as well as on other programming development and maintenance controls. Rather than looking for these in each given

application reviewed, the internal auditor should review the general systems development controls in the IT enterprise. These might be included in a general review of IT operations, as discussed in Chapter 18.

When an enterprise plans to build and launch a major in-house new or revised software application, internal audit should request the right to perform a preimplementation review of the project. Here the internal auditor can serve as an ongoing reviewer of the application development process, assessing the evolving internal controls environment and making consulting recommendations, as discussed in Chapter 28.

Preimplementation internal audit reviews are most effective for large development efforts that require an extended span of development time and consist of primarily in-house built components. Exhibit 19.3 contains internal audit procedures for a review of a new application systems development control. These control processes are closely linked with the IT general controls discussed in Chapter 18.

EXHIBIT 19.3 Internal Audit IT Applications Development Review Guidelines

1. All requests for new or revised applications should follow IT standards and receive prior authorization.
2. The application development process should include sufficient requesting user interviews to develop a firm understanding of needs.
3. All new application projects should receive a detailed statement of requirements along with a formal cost-benefit analysis.
4. Project plans should be prepared for all IT department development work as well as for individual application development projects.
5. Care should be taken to ensure that application development projects meet the long-range objectives of the enterprise.
6. Adequate time should be to scheduled for complete development of assignments.
7. The applications development process should include sufficient user interviews to obtain a full understanding of requirements.
8. Attention must be given to internal controls, audit trails, and continuity procedures.
9. Adequate resource and capacity planning should be in place to ensure that all hardware and software is sufficient when the application is placed in production.
10. Sufficient attention must be paid to backup, storage, and continuity planning for the new application.
11. Adequate controls must be installed to provide strong assurances regarding the integrity of the data processes and outputs from the application.
12. The application should be built with adequate controls for the identification and correction or processing errors.
13. All application processing data and transactions should contain strong audit trails.
14. Adequate documentation should be prepared on a technical as well as an application user level.
15. Test data should be prepared following a predetermined test plan that outlines expected results and satisfies user expectations.
16. When data is converted from an existing application, strong control procedures should be established over the conversion process.
17. If a critical application, internal audit should be given an opportunity to participate in a formal preimplementation audit.
18. The completion of the application development process should contain a formal sign-off and approval process.

Control processes should be put in place for the overall IT functions, and an internal auditor should look for them to exist in each application selected for review. Of course, today many new application development projects do not consist primarily of building tables for use with purchased software applications or building interfaces between some new purchased application and other existing components. Proper attention must be devoted to preserving internal controls and performing adequate testing in these situations. The internal audit preimplementation review approach can provide service to the enterprise.

(iii) VENDOR-SUPPLIED SOFTWARE Most IT applications today are not programmed in-house but are based on vendor-supplied software. An outside vendor supplies the basic, often Web-based, system elements. The enterprise's IT development function has to build only custom tables, file interfaces, and output report formats around the purchased application. The actual program source code for the purchased software is often protected by the vendor to prevent improper access and changes. Both the internal auditor and IT management should be concerned that the software vendor has a reputation for quality, error-free software. Often smaller entrepreneurial software suppliers can provide some very cost-effective solutions, but there can be risks in using an undercapitalized software developer. If there is any concern that the software vendor lacks stability, arrangements should be made at the time of the software purchase contract to place a version of the vendor's source code "in escrow" in the event of a vendor business failure. A bank or some other agency would hold a version of the protected source code for release to customers if the software vendor were to fail.

The decision to lease or purchase a software package is too often based on an IT manager meeting a software salesperson at a trade show, establishing a need, and purchasing the software package without a full analysis of the costs and benefits. Internal auditors often can play a strong consulting-level role in the acquisition of a new software package. There are often many internal control issues beyond what is listed in the sales brochures. Exhibit 19.4 is a checklist that an internal auditor can use when providing consulting help and reviewing the decision to purchase a major new software package. An internal auditor should have as good an understanding of the internal controls surrounding major purchased software applications as of any in-house–developed application.

Large, integrated packages such as the enterprise resource planning systems mentioned previously can have a major impact on all aspects of an enterprise. These database application packages may include production, purchasing, inventory, human resources, accounting, and all other business applications implemented as a linked series of databases. Data introduced to one application component, such as a revised standard cost for a manufactured part, will connect to other connected systems as necessary. For example, that revised standard cost will be reflected in inventory and financial systems among others.

(c) IT Application Output Components

No discussion of an application system would be complete without a description of its output components. These usually consist of output screens or updated files as well as printed reports. This is an important area to survey in an application review,

EXHIBIT 19.4 Purchased Software Internal Controls Audit Checklist

	Audit Internal Controls Procedure	Workpaper Reference
1	Determine that the requirements and objectives for the new application have been clearly approved and defined.	_____
2	Assess whether application requirements have been clearly defined and whether they can be satisfied by modification of the current application.	_____
3	If requirements call for a new application, determine whether an IT analysis has been performed to determine if it may be most cost-effective to develop in-house or to purchase.	_____
4	If a search for a potential purchased application, determine that detailed requirements have been defined through a request for proposal (RFP) approach.	_____
5	Determine that the RFP requirements clearly match the existing enterprise IT environment.	_____
6	Review the distribution procedure for RFPs to ensure that it covered all appropriate vendor candidates.	_____
7	Assess whether documentation is in place to review all vendor proposals on a consistent basis.	_____
8	For application software vendors that appear to meet preliminary requirements, determine that the software has been demonstrated effectively through demonstration testing.	_____
9	Where multiple vendors are presenting competing software products, ensure that consistent evaluation procedures are in place.	_____
10	Ensure that enterprise financial and legal resources are in place to participate in software selection.	_____
11	Check that the selected software product has adequate documentation, "help" facilities, and a regular update program in place.	_____
12	Determine that an implementation plan is in place to convert either data or an existing application to the new software application.	_____
13	Where appropriate, develop preliminary plans for CAATT procedures covering the new application.	_____
14	Establish internal audit workpaper records for new purchased software applications.	_____

as, in many instances, the controls of internal audit concern in an application are contained on the output screens or control files. Older applications produced large volumes of output reports indicating the results of the processing and any control or error problems. The sheer volume and frequency of those reports often prevented users from giving adequate attention to many control problems, and internal auditors frequently identified control concerns that users could have discovered by just reviewing their output reports.

Today's applications produce far fewer, if any paper-based output reports; most results are reported on online data-retrieval screens. In some cases, special online reports signal control problems and data errors; in others, the user is responsible for calling up the appropriate screen to review any problems. All too often, this step may be ignored and processing errors can go undetected. Internal auditors should always review the scope of application output reports and their user dispositions.

Reports or screens are not the only application outputs. Transactions or updated files typically are passed to a variety of other integrated applications. Just as a modern IT application may receive its inputs from a highly integrated set of input systems, the application may be one more link in a chain to still others. Again and always, the internal auditor should develop a good understanding of the application reviewed as well as all of its inputs and outputs.

19.2 Selecting Applications for Internal Audit Reviews

While all major IT operations and key applications should be subject to regular reviews, internal audit typically does not have the resources or time to regularly review the controls for all of its IT applications. In addition, many IT applications represent a minimal level of control risk. As part of a specific operational review or a general IT controls review, internal audit should select only the more critical applications for review. The audit process for selecting these applications should be based on the risk-based audit planning discussion in Chapter 15. Because IT applications are so critical to enterprise operations, internal auditors often receive specific requests from the audit committee or management to review specific application controls. Some of the factors that may impact internal audit's decision to select one specific application over another may include:

- **Management requests** . Management often asks internal audit to review the controls in newly installed or other significant IT applications due to reported problems or their strategic importance to the enterprise. These management requests are not always made for the correct reasons, however. For example, sales analysis reports may appear to be incorrect due to bad data submitted from a reporting division, but management may consider the incorrect reports to be a "computer problem" and request an internal audit applications review. Internal audit may not initially be aware of such user input problems and would perform normal review procedures. When internal audit is aware of such mitigating circumstances, audit test strategies should be modified prior to starting the review.
- **Preimplementation reviews of new applications.** In many instances, internal audit should become involved in reviewing new applications before they are placed in production. This is true whether the application was developed in-house or is a purchased software package. Strategies for internal audit preimplementation reviews are discussed in Section 19.6.
- **Postimplementation applications reviews.** For some critical applications, subject to a risk analysis, auditors may also want to perform a detailed applications review sometime shortly after the actual system implementation. If an application has sufficient financial and operational controls significance, internal audit may want to schedule at least limited controls reviews on an ongoing basis.
- **Internal control assessment considerations.** Chapter 4 discussed the need for evaluating and testing internal controls as part of the Sarbanes-Oxley (SOx) Section 404 process, and an IT application controls assessment is an important part of that overall Section 404 evaluation. The results of internal audit's understanding, documenting, and testing of specific IT applications controls provides a basis for the external auditors SOx attestation processes.

- **Other audit application selection criteria.** There are many other reasons why internal auditors may select one application over another for a detailed, internal controls–oriented review. Besides the reasons discussed here and in Chapter 15, their selections may be based on these considerations:
  - Does the application control significant assets?
  - Does the application's performance represent a significant risk exposure to the enterprise?
  - Is the application a strategic system for enterprise decision making?
  - Does the application support a function that will be reviewed later as a scheduled internal audit review?
  - Have significant changes been made to the application?
  - Have there been significant personnel changes in the departments or functions using the application?

  Internal audit typically is faced with requests for reviews of a large number of applications at any time, and care should be taken in documenting the reasons for selecting one application over another. This will help if internal audit is questioned subsequent to completing a series of reviews. Audits of the controls over representative IT applications are sometimes included as part of a general controls review of the IT function. Internal audit should develop a detailed understanding of the general controls surrounding IT operations, as discussed in Chapter 18, and then review the controls surrounding one or more selected applications.

Internal auditors often perform reviews of the specific applications that support an overall functional area. For example, internal audit may schedule a combined operational and financial review of the purchasing department. This may also be the appropriate time to review the application controls for the major automated purchasing systems supporting that department. In this integrated audit approach, internal auditors can concentrate on the more technical issues surrounding the applications and on other supporting operational controls.

19.3 Preliminary Steps to Performing Applications Controls Reviews

Once an application has been selected for review, internal audit should gain an understanding of the purpose or objectives, the technology approaches used, and the relationship of that application to other related automated or significant processes. It may be necessary for the assigned internal auditor to do some background reading and study special technical aspects of that application. Often this auditor understanding can be accomplished through reviews of past audit workpapers, interviews with IT and user personnel, and reviews of applications documentation. While prior audit workpapers can be very helpful and the interview process will allow an auditor to ask relevant controls-related questions, a review of applications documentation is often a useful first step in evaluating the controls over an IT application. Chapter 16 discusses preparing and creating effective audit workpapers. As an early step in this review process, internal audit should perform a walk-through of the application to better understand how it works and how its controls function. These preliminary steps will allow an internal auditor to develop specific audit tests of the application's more significant controls.

In the early days of enterprise-developed IT applications, documentation often consisted of detailed system and sometimes manually prepared flowcharts with supporting record layouts and little else. This helped the programmer but was of little use to application users or internal auditors attempting to understand the application's controls. In addition, because these early flowcharts were often hand-prepared, they quickly became out of date. When one relatively small change was added to a complex system flowchart, designers were often reluctant to redraw charts. Although they may have remembered the changes, other interested persons reviewing this documentation, such as internal auditors, would not be aware of them.

Over time, applications documentation evolved into a more text- and functional chart–oriented format. Decision tables and logic charts described the functions of individual programs while text described the overall system. Although this type of documentation was more functional and less technical, it also had a tendency to become out of date quickly. Programmers and system designers often would not take the time to incorporate later changes into this systems documentation. Today, powerful documentation tools such as flowchart generators are available. A real strength of these automated documentation tools is that detailed flowcharts can be combined into summarized versions with changes introduced on one chart updating all others.

Internal audit can expect to find various types and quantities of applications documentation depending on the relative age and complexity of the application to be reviewed. Due to poor IT management procedures, complex in-house–developed applications sometimes have very limited documentation. The published documentation covering other vendor-supplied applications, however, often includes many dozens of volumes of descriptive text. Users treat such documentation as almost encyclopedic reference materials. A review of the published documentation should be a first step to gaining an audit understanding of an application. If aspects of the documentation are missing or out of date, the internal auditor will probably have a finding at the conclusion of the review. However, this lack of documentation should not necessarily prevent an internal auditor from performing an application review. When performing the review, internal audit should normally look for these documentation elements:

- **Systems development methodology (SDM) initiating documents.** These refer to initial project requests, any cost/benefit justifications, and the general systems design requirements. Although many initial assumptions may have changed during the systems design and implementation process, these documents often will help internal audit understand why the application was designed and controlled in the manner it is.
- **Functional design specification** . This documentation should describe the application in some detail. Each of the program elements, database specifications, and systems controls should be described. If major changes have been made to the application since its original implementation, these changes should also be reflected in the design documentation. Their purpose is to allow an IT analyst to make changes or respond to user questions regarding the application.
- **Program change histories.** There should be some type of log or documented record listing all program changes within an application. Some IT departments keep this with the applications documentation while others maintain it in a central file cross-referenced to the program source code. This type of

documentation is an essential element to control program changes; it also provides internal audit some feel for the application's relative stability. A large number of ongoing change requests for a given application may mean that the application system is not achieving user objectives. Revision service support controls should follow the IT infrastructure library (ITIL) best practices as discussed in Chapter 18.

- **User documentation manuals.** Along with technical documentation, appropriate user documentation should be available for any application. In a modern, Web-based system, much of this user documentation may be in the form of "HELP" or "READ ME" online screens. However, this documentation should be sufficiently comprehensive to answer user questions. It should also be supported by evidence of a user training program, as appropriate.

Internal audit should review selected application documentation to gain an understanding for the controls to be reviewed and perhaps use these materials to develop questions for later interviews. Copies of key or representative sections should also be taken for workpaper documentation. However, internal audit should normally not attempt to copy the entire documentation file for workpaper purposes. Internal auditors often do this; it adds considerable bulk to workpaper files but does little to accomplish audit objectives.

(a) Conducting an Application Walk-Through

Once internal audit has reviewed prior workpapers and the applications documentation, and interviewed users and IT personnel to clarify any questions raised through the documentation review, a next step is to verify internal audit's understanding of the application by a *walk-through* review. For an IT application, a walk-through review is the same type of internal audit process as an initial review of an operational facility where the auditor tours a facility, such as a production floor. The purpose of this walk-through is to confirm internal audit's general understanding about how the operational facility and IT application operates. During the walk-through, internal audit preliminarily tests application controls through sample transactions.

As an example of an application walk-through process, assume that internal audit has been asked to review the controls over an older in-house–developed accounts payable application operating on an in-house server system. The enterprise is a manufacturing firm with other fairly sophisticated IT applications. This accounts payable application was installed several years before and was never reviewed when it was under development. Now management has asked internal audit to review the application's internal controls as part of a SOx Section 404 review. Based on the review of application documentation, internal audit has determined that the application receives inputs from these sources:

- Purchase order commitments from the manufacturing material requirements planning purchasing system
- Notifications of goods received from the materials-receiving system
- Various online terminal payment transactions for indirect goods and services that are not recorded through the materials-receiving system
- Payment approval transactions entered through an input screen
- Miscellaneous payables journal transactions entered as batch data

EXHIBIT 19.5 Applications Walk-Through Internal Auditor Steps

1. Develop a general understanding of the application, its inputs, outputs, and any procedures requiring manual or other system interactions.
2. For an application with a large number of steps requiring manual processing procedures, select a sample of key transaction types to be processed from a normal production cycle. For workpaper documentation purposes, document identifying control numbers or other characteristics to tract transaction through application processes.
3. Observe or use software tools to monitor the processing of each module or workstation step, noting situations where the walk-through transaction is:
   a. Inputs to another application or supporting process are passed on through the node processing module
   b. Held for further cycles in process or rejected as errors during the specific processing module
4. Follow selected transactions through each processing module step, documenting instances where the documented control procedures are not being followed or where the transaction causes application errors or manual operator difficulties.
5. At the end of the walk-through, discuss with appropriate IT or user administrators any unusual or unexpected problems, and document internal control status.
6. For an automated application with no paper trail, follow essentially the same procedures but make inquiries and use software query tools to determine that the application is processing with appropriate controls and as expected.

Application data are recorded on a relational database along with tables of values for validating purchase terms, including the calculation of any purchase discounts. Based on the review of documentation, application outputs include the accounts payable electronic fund transfer transactions as well as paper checks, transactions to the general ledger and cost accounting applications, and various control and accounting summary screens and reports.

The prime system users are personnel from general accounting and the purchasing department, who set up automatic vendor payments under preagreed terms. As an example, Exhibit 19.5 describes this applications walk-through and also will a be referenced in other examples in this chapter. The steps to performing an application walk-through for the example accounts payable application are described next.

Step 1. Briefl describe the application in the audit workpapers. Based on internal audit's review of the applications documentation, prepare a brief description of the application for later inclusion in the audit workpapers. This workpaper documentation follows the general format of the walk-through description except there should be greater detail, identifying key subsystems, input screen formats, key data file names, and output report formats. (For a discussion of internal audit workpapers, see Chapter 16.)

Step 2. Develop a block diagram or flowchar description of the application from the Step 1 description. This diagram represents an abbreviated auditor-level systems description or functional-level flowchart for the application. It should reflect the Step 1 description and also illustrate some application flow concepts. This typically hand-drawn document will help increase auditor understanding of the application reviewed.

Step 3. Select key application transactions. Based on the auditor's understanding, one or several representative transactions should be selected to walk or to trace through the application. This selection can be based on discussions with users and fellow members of the audit team. In this example of an accounts payable system, the auditor may select automated transactions that the receiving system should match against the payables purchase order records to initiate payment.

Step 4. Walk through a selected transaction through the system processes. In older days of manual or simpler IT applications, a walk-through amounted to just what the words say: An auditor would take an input transaction document and would walk it through each of the clerical desks or steps normally used to verify the processing procedures. In a modern application, this walk-through process typically requires recording screen shot prints of a transaction as it is entered into a terminal and then following the transaction through its subsequent steps. In this accounts payable example, the walk-through transaction is a receiving report entry indicating that a valid open purchase commitment had been received. Internal audit would then review the open commitments module of the system to determine whether the transaction was recorded on a transaction report or screen. Then the transaction is traced to a properly computed accounts payable check or to a funds-transfer transaction and then to general ledger system transactions for the correct amount.

This type of applications testing is often called *compliance testing*. That is, internal audit is verifying that the application is operating in compliance with preestablished control procedures. Verifying that all accounts payable checks have been input to the general ledger through a comparison of account balances or other methods is called *substantive testing,* or a test of financial statement balances. Tests in support of SOx Section 404 controls typically tie a single item test to financial statement general ledger accounts.

Step 5. Modify the auditor's understanding of the application as required. Since the purpose of an application walk-through is to develop a basic understanding of its functions and controls, a walk-through review does not allow internal audit to determine whether *all* transactions are working as described. However, if internal audit discovers that the selected walk-through transactions are not working as assumed, the preliminary auditor-prepared application documentation may need to be revised. Once revised, internal audit may want to repeat the last steps to determine that internal audit has a proper understanding of system transaction flows.

The walk-through allows internal audit to gain a preliminary understanding not only of the application and its controls but also of its relationship with other automated systems. Limited compliance testing allows the internal auditor to confirm that the application is operating as described. While not a substitute for detailed, substantive application testing, the walk-through allows an internal auditor to identify major control weaknesses as well as to gain a sufficient understanding of the application to define control objectives for subsequent, detailed audit testing and evaluation procedures.

(b) Developing Application Control Objectives

After the review of documentation and walk-through compliance testing, an internal auditor should develop detailed audit objectives and procedures for completing the application review. This depends on the type of review planned, the characteristics of the application, and the results of the preliminary review steps. A given review might concern the level of control risk and the ability of the application to support financial statements correctly. The procedures associated with these audit objectives would be tests of the financial statement balances built up from detailed application transactions.

An internal auditor could also have other objectives in reviewing an IT application. Management may have asked internal audit to review it to determine if user personnel have received sufficient training or to review another related application to determine if accounts payable discount and interest calculations are correctly performed. The walk-through compliance testing may have identified significant problems, and the auditor may want to do little more than to confirm those preliminary but troubling observations. Before proceeding any further with the review, the internal auditor should confirm or revise the specific review objectives.

The review objectives for a specific application should be clearly defined. The responsible internal auditor might wish to summarize these objectives for the review and approval by appropriate members of management. This may help prevent an internal auditor from devoting resources to testing an area not considered significant. In the accounts payable system just mentioned, an internal auditor may have established several specific objectives for this review:

- The accounts payable system should have adequate internal controls, such that all receipts recorded from the receiving system are correctly matched to vendor files before the preparation of disbursements.
- Vendor terms should be correctly computed with controls to eliminate potential duplicate payments.
- Controls should be in place to prevent or at least flag improper or unusual disbursements.
- All systems-generated disbursements should be recorded on general ledger files using correct account numbers and other descriptive codes.

Depending on management's direction, internal audit might develop other objectives for performing such a review. For example, the review could focus on database integrity or on control procedures over miscellaneous disbursements. Any review may have multiple objectives. For example, if management had asked internal audit to review the accounts payable system to assure that no illegal or improper payments have been made, internal audit would probably also want to add a general objective to assess control risk and to determine that the system of internal controls is adequate.

Before starting any detailed applications review, internal audit should document the specific objectives of the review and discuss them with the management requesting the review to determine if the planned review approach is on target and will satisfy the audit request. This same procedure should take place even if the review has been initiated by the audit department as part of a total review of an IT function. Exhibit 19.6 contains suggested control objectives for an IT applications review.

EXHIBIT 19.6 Control Objectives for an IT Application Review

1. Develop a general understanding of the application to be reviewed: its principal business purposes, inputs, outputs, and the technology environment.
2. Based on the general understanding of the application, develop a general process flowchart that identifies key decision points, inputs, outputs, and internal controls.
3. Develop an understanding of the general controls surrounding the application and its processing environment, with an emphasis on ITIL service support and service delivery general controls. (See Chapter 18.)
4. Discuss the application and its performance with key system users and IT to understand any concerns or outstanding issues regarding the application.
5. Develop a testing plan for the application that emphasizes:
   a. Identification of significant transactions, accounting and business-related controls within and surrounding the application's environment.
   b. Identification of control objectives covering each significant control as well as areas of concern that should satisfy the auditor that key controls are effective.
   c. Development of testing and sampling approaches for each key control.
6. Gather evidence to perform tests of identified key controls, including:
   a. Copies of key files and extracts of transactions to reperform application functions.
   b. Special application transaction to test key or critical application controls.
   c. CAATT procedures or package software functions to review application transactions and special functions.
   d. Manual or paper-based documentation to support the applications controls testing.
7. Schedule and perform tests of key application controls using the test materials gathered.
8. Evaluate all test results in a pass/fail context, and communicate testing results with key systems users and IT to verify and validate the testing approach and its results.
9. Maintain copies of all testing plans and evidence, documenting the results in internal audit workpapers.
10. Develop an appropriate corrective action plan, where appropriate, to correct any problems encountered in the testing or application review.

19.4 Completing the IT Application's Controls Audit

Detailed IT application audit procedures are usually more difficult to define than an internal audit's general objectives. The procedures vary and depend on whether (1) the application primarily uses purchased or in-house–developed software components; (2) the application is integrated with others or is a separate process; (3) it uses Web-based service providers, client-server or older, legacy computer system methods; and (4) whether its controls are largely automated or require extensive human intervention actions. The exact nature of an application can also vary considerably. Although the emphasis of internal audits was once primarily over controls in accounting-related applications, today's internal auditors should review applications over other areas as well, such as manufacturing resource planning or loan portfolio analysis. Any of these areas require knowledge of the application's specific attributes and the supporting technologies. That is, an internal auditor should understand how the application works by first documenting the IT applications, then defining specific audit test objectives, and finally performing a series of audit tests to verify that the application controls are in place and working as expected.

Besides the review of documentation and the walk-through, discussions with key user personnel and responsible systems personnel can aid the auditor's

understanding. The amount of effort spent here depends both on the type of application reviewed and the number of users who can be of help. For example, a capital budgeting decision support application will probably have a small group of key users who have a thorough understanding of its procedures. A logistical support system, such as factory floor data collection, may be used by a large group, and it may be difficult to identify the key system users.

The next step is to complete the documentation of the application for audit purposes. Internal audit should have been making workpaper notes throughout. The documentation procedure here is largely one of summarization where workpapers describe the understanding gained and include notes for potential follow-up review work.

(a) Clarifying and Testing Audit Internal Control Objectives

The previous section discussed the importance of establishing test objectives as part of an applications review—the types of internal controls an auditor would expect to be in place for an application. The next step of clarifying these review objectives is often a major area where internal audit has been known to fail. Management may expect internal audit to review accounting controls, but internal audit's review may only have emphasized logical security controls, paying less attention to other established control objectives. This misunderstanding of audit objectives becomes especially critical when the review is not typically in the auditor's usual realm of accounting applications. For example, if management has asked internal audit to review a new manufacturing resource planning system, its objectives could include validating internal accounting controls, reviewing for materials parts flow efficiencies, checking for system compliance with applicable regulations, or a combination of these. These objectives should be summarized by internal audit into a brief statement and discussed with both audit management and applications-user management.

Although the need for a clear statement of review objectives may appear an obvious early step, auditors often omit it. Of course, the objectives of an applications review may change if internal audit encounters evidence of other control problems during a review that would suggest audit scope or procedure changes. In a manufacturing resource review, for example, the initial objective of affirming the adequacy of the application's internal controls might change to one of fraud detection if potentially invalid transactions were encountered.

Internal audit should next test the key control points within the application. Having already done limited compliance testing as part of gaining an understanding and the walk-through, these test procedures can now be expanded to make a more definitive assessment of the application's controls. In older and simpler batch-oriented systems, this task was fairly easy. Internal audit looked for input data acceptance controls, for any computer-processing decision points, and for output data verification controls. Since only a few processes were associated with such an older batch application, this identification of test procedures could be accomplished today with minimal analysis. Modern applications with online updating, close integration with other applications, and sophisticated programming techniques all combine to make identifying test procedures difficult. Other factors include:

- Inputs to the application may have been generated by external sources, such as Web linkages, or from other applications at partner enterprises.
- Controls once performed by data input personnel are now built into programs.

EXHIBIT 19.7 Sample IT Application Audit Test Procedures

These test procedures are ones that an internal auditor might use when assessing IT application internal controls. Based on the nature and objectives of the application, these may not apply to all applications. The auditor needs to have a detailed understanding of the application and its key internal controls before developing a test plan.

- **Foot key files** Using available purchased software tools or CAATTs, determine key data file values and report total foot to supporting totals and appropriate totals and balances are correct.
- **Test key calculations.** Using sample transactions, determine that results and totals are correct as predicted.
- **Consider running special audit-only updates.** Prepare a set of transactions covering all key aspects of the application and arrange for a special, audit-only update. Review the results of the update for controls and processing accuracy, and remove the special audit-updated from the production cycle.
- **Perform transaction balancing.** Using the transaction totals from a production process, independently calculate and reconcile audit control totals to reported application totals from the same cycle.
- **Review application logical security.** Review the application's embedded security levels to determine that all users are granted proper levels of read-and-write access.
- **Document internal controls.** Test for controls of key documents (ID numbers, etc.) to determine that updates can be traced back to their point of origination.
- **Review for unauthorized changes.** Review program library update logs, and determine that application program versions in production libraries are the same as those retained in documentation files.
- **Assess contingency planning provisions.** Depending on audit risk, review the continuity and contingency planning provisions and the results of any testing processes.

- Modern optical scanning input devices and output documents with multidimensional bar codes make visual inspection difficult.
- Database files may be shared with other applications, making it difficult to determine where a change or transaction originated.
- The application may make extensive use of Web interfaces and will appear paperless to internal audit.

There are numerous other reasons why an internal auditor may have difficulty initially identifying IT application audit test procedures. The application's description, along with key user discussions, should help to identify some of these controls. As a rule of thumb, an internal auditor should look for points where system logic or control decisions are made within an application and then develop test procedures to verify that those decision points are correct. These points represent the key controls within an application, such as checks on the completeness of transactions or the accuracy of calculations. Exhibit 19.7 lists some typical test procedures oriented to more modern client-server applications.

(i) TESTS OF APPLICATION INPUTS AND OUTPUTS In the very early days of IT auditing, many audit-related tests were little more than checks to verify that all inputs to a program were accounted for correctly and that the correct number of output transactions was produced based on these inputs. For example, consider an auditor's review of an automated payroll system. The internal auditor would test to determine

that all time cards input were either accepted or rejected and that the number of output payroll checks produced could be reconciled to those system input time cards. This is a test of system inputs and outputs.

Although automated applications have become much more complex, many audit test procedures today are little more than those same tests of inputs and outputs. An internal auditor should examine the outputs generated from an application, such as invoices produced by a billing system, to determine that the input data and automated computations are correct. This type of audit test is limited in nature and will not cover all transactions or functions within an application.

The purpose of a control risk assessment or compliance test is to determine if application controls appear to be working. If all transactions or all data are to be reviewed, substantive testing procedures or tests of financial statement balances, as discussed in Chapter 9, should be used. The extent of this testing depends on the audit objectives. For example, an external auditor will tend to perform compliance tests over those aspects of an application that cover financial statement–related internal accounting controls. An internal auditor may also want to perform compliance tests over other areas, such as the efficiency of administrative controls.

For older applications, tests of inputs and outputs are often quite easy to perform. The auditor would select a sample of input transactions and then determine if the number of inputs was equal to the count of processed items plus any rejected or error items. This type of audit test is not nearly as easy for today's applications, where the auditor often will not encounter a one-to-one relationship between inputs and outputs. Test transaction approaches, to be discussed, are often much easier to perform and even more meaningful. Nevertheless, tests of inputs and outputs are sometimes useful for reviews of applications. Audit procedures for an example automated purchasing application compliance tests are outlined in Exhibit 19.8.

EXHIBIT 19.8 Automated Purchasing System Compliance Tests Example

1. Select a series of purchase orders generated by the application reviewed, and trace them back to either the requirements generated by the manufacturing system or by authorized manual purchase inputs, determining that all new purchase orders have been properly authorized.
2. From the sample from item 1, trace the purchase orders selected back to established records for vendor terms and prices, resolving any differences.
3. Select and trace a cycle of automated purchase order to EDI or Web control logs to determine that all documents were transmitted without error and on a timely basis.
4. Using a sample of purchase orders received either from EDI or the Web log, determine that vendors are documented through current, signed purchase agreements.
5. Select a sample of receiving reports, and determine that the application is working properly by matching receipts to open purchase orders and accounts payable records.
6. Select a sample of recent accounts payable vouchers and any actual checks generated for parts and materials, tracing the payments to valid receiving reports and purchase orders.
7. Using sample transactions that were either held on receipt for noncompliance with terms or improper timing, verify that transactions are handled correctly and per established procedures.
8. Balance a full cycle of purchase transactions, from the manufacturing system providing inputs to the control logs over EDI, Web log, and printed purchase order documents.

(ii) **TEST TRANSACTION EVALUATION APPROACHES** Using this example application, the internal auditor should ascertain that input transactions are processed correctly. For example, when reviewing a plant floor manufacturing application, an internal auditor might record several shop materials transactions as they are entered on manufacturing floor terminals. After an overnight processing cycle, the auditor can verify that those transactions have correctly made adjustments to inventory records and that work-in-process cost reports have been properly updated. This verification can take place by reviewing special retrieval reports against data files. As part of the test transaction process, an auditor can also test whether error-screening controls are operating as described. The emphasis here should be on the testing of the error-verification routines within the application. Internal audit can select transactions input to an application that appear to be invalid and then trace them through the application to determine whether they have been properly reported on exception reports. Internal audit can also consider submitting test error transactions to a system to verify that they are being rejected properly by the application.

(iii) **OTHER APPLICATION-REVIEW TECHNIQUES** The computer-assisted audit tool and techniques (CAATT) processes discussed in Chapter 21 can be useful in reviewing application controls. All too often, internal auditors use these tools to test some accounting control, such as an accounts receivable billing calculation, but often do not to evaluate other application controls. Audit software can match files from different periods, identify unusual data items, perform footings and recalculations, and simulate selected functions of an application. Other useful techniques are:

- **Reperformance of application functions or calculations.** This type of test is applicable for both the automated and the manual aspects of application systems. For example, if a fixed-assets application performs automatic depreciation calculations, internal audit can use CAATT processes to recalculate depreciation values for selected transactions as a compliance test.
- **Reviews of program source code.** For in-house–developed applications, internal audit can verify that a certain logic check is performed within a program by verifying the source code. However, this type of compliance test should be used only with the *greatest amount of caution*. Because of the potential complexity of trying to read and understand program source code, it is very easy to miss a program branch around the area being tested. Specialized programs are available to compare program source code with the compiled versions in production libraries.
- **Continuous audit monitoring approaches.** Internal audit can sometimes arrange to build embedded audit procedures into production applications to allow those applications to flag control or other application exception problems. These techniques also are discussed in Chapter 21 on CAATTs, This approach goes beyond just auditing an application and helps to make it self-auditable.
- **Observation of procedures.** Observations may be useful when reviewing both automated applications and manual processes. For example, a remote workstation receiving downloaded data from a central system may require extensive manual procedures in order to make the proper download connection. Internal audit can observe this on a test basis to determine if these manual procedures are being performed correctly.

(b) Completing the Application Controls Review

Although compliance tests are powerful methods to test application controls, this level of assurance is not absolute. There is a risk that an internal auditor may test an application control and find it to be working when, in fact, it does not normally work as tested. Because of the false results that could be associated with such compliance tests, internal audit should always be careful to condition reports here with a comment about the risks of incorrect results due to limited audit tests. Sometimes the controls tested do not appear to be working correctly because internal audit does not understand some aspects of the application. Internal audit may want to review the application description and its controls with IT and users to verify that they are correct. Based on such a review, it may be necessary to revise internal audit's understanding of application controls and then to reperform the audit risk assessment procedures.

If internal audit finds that, through compliance testing, the application controls are not working, it probably will have to report these findings. The nature of this report very much depends on the severity of the control weaknesses and the type of review. For example, if the application is being reviewed at the request of the external auditors, the identified control weaknesses may prevent them from placing any reliance on the financial results produced by the application. If the control weaknesses are primarily efficiency related or operational, internal audit may want to just report them to IT management for future corrective action.

Applications can be primarily financial or operational. They can be implemented using purchased software, can be custom-developed applications located on in-house systems with extensive database and telecommunications facilities, or can operate in a client-server environment or exist in numerous other variations. As noted, this diversity makes it difficult to provide just one set of audit procedures for all applications. While internal audit can develop a general approach to reviewing most data-processing applications, it is usually necessary to tailor that approach to the specific features of a given application. The next section describes how an internal auditor might perform a review of a capital budgeting application operating in a client-server environment with telecommunication links through a network to a larger server.

19.5 Application Review Example: Client-Server Budgeting System

As an application review example, assume internal audit has been asked to review the controls over an in-house client-server architecture capital budgeting system. The financial planning department has developed the capital budgeting analysis portion of the application using a popular desktop spreadsheet software package. Although built around a purchased software spreadsheet package, the users have coded a series of macro instructions for running the programs. The workstation portion of the system communicates with a server file containing mainframe budgeting system data.

Internal audit has been asked by management to review general controls over both local networks and their client-server computer operations. Following the audit procedures in Chapter 18, internal audit found that general controls in these areas were adequate. That is, users documented their desktop applications; adequate backups of files and programs were performed on server files; password procedures

limited access to only authorized personnel; and other good control procedures were followed. Among internal audit's recommendations was to place stronger controls over telecommunications access to the local network and to install virus-scanning procedures.

Some time after that general controls review, this capital budgeting system was implemented on the administrative office network. Because this system provides direct input to the corporate budgeting system, management has asked internal audit to review its application controls. After discussing this review request with senior and IT management, internal audit developed these review objectives:

- The spreadsheet capital budgeting system should have good internal accounting controls.
- The application should properly make capital budgeting decisions based on both the parameters input to the system and programmed macro formulas.
- The system should provide accurate inputs to the central or corporate budgeting system through the local file server.
- The capital budgeting system should promote efficiency within the financial planning department.

These represent the general format for internal audit objectives for this type of application. Often management does not state its aims quite so clearly but may be looking for performance or features objectives. It is the responsibility of internal audit to listen to management's requests and to translate them to review objectives.

(a) Reviewing Capital Budgeting System Documentation

Internal audit's first step should be to review the documentation available for this example application. Since the application is built around a commercial desktop software product, internal audit might expect to find some of these items:

- Documentation for the capital budgeting software package, including spreadsheet macro procedures and formulas.
- Procedures for uploading capital budget data to the central system budgeting application through network server files as well as procedures for accepting the input data to the mainframe IT function.
- Procedures to ensure the integrity of the data resident on server files. Internal audit should expect to find documentation covering the software product used, the interfaces with other applications, and the necessary manual procedures.

Internal audit should review these materials to determine that they are complete and to gain a general understanding of the overall application. Then, after reviewing this documentation and discussing it with its financial planning users, internal audit should describe the application for audit workpaper documentation purposes. Since the application is built around a spreadsheet software product, this description primarily covers its manual interfaces. Control descriptions over file server applications and their network connections to client systems have been covered as part of the general controls review. Auditors often find it convenient to describe such an application in the form of a flowchart, although a written description may be adequate. The purpose of this type of description is to provide internal audit with workpaper

documentation of the application and to provide a basis for the identification of significant control points.

(b) Identifying Capital Budgeting Application Key Controls

Although a rather simple but compact application, this example capital budgeting application has some critical control points. For example, if the spreadsheet macro procedures are incorrectly calculating capital costs, present values, and related factors, management may very well take incorrect actions regarding investment decisions. If data are incorrectly transmitted to the mainframe budgeting system, financial statement records may be incorrect. If the application is not documented properly, a change of key users in the financial-planning department may make the system nearly inoperable.

Based on internal audit's understanding of this example system, key system controls are now defined and documented. Here, because internal audit has recently performed a general controls review, it is not necessary to reconsider those controls during the applications review. The audit review procedures can now be developed similar to those shown in Exhibit 19.9.

EXHIBIT 19.9 Capital Budgeting Application Input and Output Audit Tests

1. Develop a detailed understanding of all significant application input transactions—their nature, timing, and source.
2. Develop a strong understanding of transaction error correction procedures, both the nature of the tables or rules used for verification as well in any built-in system logic; determine that formal turnaround procedures exist to control any initial error items.
3. Using documentation or database descriptions, trace all input to output data flows with the application showing how many input elements (e.g., orders from the inventory application) will change or modify other system elements. Document this understanding in workpapers through audit data process flow diagrams (see Chapter 16).
4. Determine that controls exist for comparing the number of items input to those that have been either accepted or rejected; review error identification procedures to determine if users can easily understand the cause and nature of any errors.
5. Review procedures for the correction and resubmission of rejected items; determine if errors are held in suspense files for analysis and corrective actions.
6. Develop a detailed understanding of all significant system output control totals, and review the nature of supporting controls for a selected single application update processing cycle and from cycle to cycle.
7. Select an input update cycle for review, and determine if the number of items input, less any rejected errors, ties to application output control totals.
8. For the test cycle selected for review, determine that all error items from the cycle have been corrected, resubmitted, or received proper disposition.
9. Review control totals in the subsequent processing cycle to determine if file totals have remained consistent from one cycle to the next, investigating any discrepancies.
10. Review existing error suspense files to ascertain that all error items have been investigated and corrected in a timely manner; investigate any items remaining in the error cycle to determine reasons for any delays.
11. Review any preliminary concerns or errors with IT and responsible management to make any necessary changes to audit test procedures.
12. Document all testing activity in workpapers.

(c) Performing Application Tests of Compliance

For the final step in this application review, internal audit should perform tests of the established audit procedures. Depending on management's and internal audit's relative interest in the application, it may not be necessary to test all of the controls as listed. Many are related to one another. If no problems or weaknesses are identified in one control area, internal audit may decide to pass on the related control areas. Some of the tests of application controls might include:

- **Reperformance of computations.** The capital budgeting process is based on some very specific computations, such as the estimation of the present value of future cash flows based on discount factors. Using another spreadsheet tool or even a desk calculator, internal audit could select one or several present value computations generated by the system and recalculate them to determine the reasonableness of system processes. Any major differences should be resolved.
- **Comparison of transactions.** Internal audit can select several sets of application budget schedules and trace them through the file server budget system to determine that they have been correctly transmitted.
- **Proper approval of transactions.** Before any system-generated budget schedule is transmitted to the central budget system, it should have had proper management approvals. Internal audit should select a sample of them for review.

Numerous other similar compliance tests can be performed for such an application. The imaginative internal auditor will be able to perform these depending on the nature of the audit and the objectives of management. Control weaknesses should be reported to management for corrective action.

19.6 Auditing Applications under Development

Many internal auditors recognize that it is much more efficient to review an IT application for its internal controls while it is being developed and implemented rather than after it has been placed into production. The role of the internal auditor here is similar to that of a building inspector reviewing a new construction project. It would be difficult to make constructive recommendations regarding the completed building. Even if some problems were found, the inspector would be under considerable pressure not to identify problems that would require significant portions of the building to be torn down and rebuilt. Rather, the building inspector identifies problems during construction and suggests how they can be corrected before completion. Similar to that building inspector, the effective internal auditor should also suggest corrective actions to improve system controls along the way. It is easier to implement changes during an applications implementation process than after it has been completed and the system placed into production.

To continue with the analogy, an internal auditor must be careful not to take responsibility for *designing* the new application's controls. The building inspector points out problems but certainly does not take responsibility for their construction. The discussion on the foundations of internal auditing, in Chapter 1, emphasize that it is internal audit's task to review and recommend but not to design or build the controls in any area reviewed. When reviewing new applications under development,

an internal auditor should point out internal control weaknesses to the application developers but only recommend they implement those recommendations.

Application development groups, user management, and auditors all tend to agree that, in reviewing new IT applications under development, internal audit provides another set of eyes to look at the new and soon-to-be-implemented application. This section offers approaches to reviewing new applications under development as well as a discussion of some of the pitfalls internal audit may encounter when attempting to audit them.

(a) Objectives and Obstacles of Preimplementation Auditing

When the concept of preimplementation reviews was first proposed by the then new profession of EDP auditors in the early 1970s, many traditional internal auditors often were opposed to the approach. Traditionalists argued that if an auditor reviewed an application in advance of its implementation, it would be difficult to come back later and review that same application after implementation. The argument was that if an internal auditor had "blessed" the internal controls of a system under development, how could that same auditor come back later and perform a critical review? Over the years, internal auditors have grown to accept preimplementation reviews, acting as auditors and not consultants. Internal auditors, however, face four major obstacles when reviewing new applications under development:

1. **Them versus us attitudes** . Although internal audit and general management may both accept the concept, IT management often may express a wariness or even resentment when internal audit announces its plan to review an application that is under development and still has many details to be worked out. The announcement "Hello, I'm from internal audit, and I am here to help you" may not be received all that favorably here. Good preimplementation review procedures can establish respect for internal audit's role and add value in the development process. An internal auditor who spends many hours reviewing a complex new application with some potential control-related issues and who concludes only with a "Documentation needs to be improved" recommendation will not be viewed as having added much value to the process.
2. **Internal auditor role problems.** The auditor's role must be clearly understood by all parties and might be defined as one of these:
   - **Extra member of the implementation team.** The systems design team invites the auditor to various design review meetings. However, the internal auditor will be more of an observer than a typical member of the design team. The auditor's objective is to gather data regarding key controls and processing procedures for a subsequent audit report.
   - **Specialized consultant.** Sometimes an internal auditor can become so involved in the systems design and development process that he or she is viewed as just another design team consultant making recommendations during the course of the implementation process. Internal audit should take care not to be viewed in that light. Following the standards for an internal auditor as an enterprise consultant, discussed in Chapter 28, an internal auditor should act primarily as an independent reviewer providing help to the team, not as a specialized consultant who is part of the design process.

- **Internal controls expert.** Internal audit should always make certain that a review of internal controls is included in the new project. However, the auditor should not be the primary designer of those controls. Otherwise, he or she may have problems reviewing the completed application and its controls at some later date.
- **Occupant of the extra chair.** Sometimes an internal auditor does not do a proper level of preparatory work as part of a preimplementation review. However, systems management may request an auditor to review various materials and attend design review meetings. An internal auditor who does not prepare but simply attends these meetings provides no real contributions. Nevertheless, if problems occur in the future, management may say "But internal audit was there!"
- **State-of-the-art awareness needs.** New systems applications often involve new technologies or business processes. A general understanding of new technologies may require additional auditor homework, to read vendor manuals and other documentation.
- **Many and varied preimplementation candidates.** The typical larger enterprise may have a significant number of new application projects that are potential candidates for preimplementation reviews. These projects will all have different start times, durations, and completion dates. An internal auditor needs to perform an ongoing risk assessment to select the most appropriate new review candidates.

Despite these potential obstacles, there are strong reasons for an internal audit function to become actively involved in preimplementaion reviews of major or critical new applications. This is particularly true in today's era of major enterprise-wide applications that require detailed planning and testing in all areas of the enterprise.

(b) Preimplementation Review Objectives

A key objective of application preimplementation auditing is to identify and recommend controls improvements such that they can be potentially installed during the applications-development process. However, rather than just assuming that a new IT project is a given and then reviewing its controls, internal audit should also have an objective of reviewing the justification and definition of the new development project. There should be a good project management system in place that properly plans development steps and measures actual progress against those planned steps. For more major projects, internal audit can evaluate the adequacy of project development controls used for the particular application. This preimplementation phase also is an excellent time for an internal auditor to gain an understanding of the new application sufficient to design future automated audit tests and to define the CAATTs, as discussed in Chapter 21. Whether it is an in-house–developed application or the implementation of a vendor package, internal auditors reviewing new applications under development should gain an overall understanding of all aspects of that application project.

In addition, some internal auditors are faced with a statutory requirement for reviewing new applications under development. Several U.S. states and other countries have legislation requiring that all new significant state agency applications be

reviewed by their internal audit departments for controls prior to implementation. Auditors in state governments can expect such legislation to appear in their own states in the future.

(c) Preimplementation Review Problems

Preimplementation reviews often present internal audit with some very serious implementation problems, including a frequent challenge of too many review candidates, given limited internal audit resources. Internal auditors sometimes make the mistake of announcing their intention of reviewing *all* new applications and all major modifications prior to their implementation. In a larger enterprise, there may be dozens or even hundreds of user requests for new or major revision applications projects initiated regularly. Internal audit will have no time for comprehensive preimplementation reviews and have only time for little more than nominal rubber-stamp approval signatures. To overcome these difficulties, internal audit should consider these points:

- **Selecting the right applications to review.** Auditors are faced with the problem of selecting only those applications of audit significance. Rather than rely on a simple value judgment or an arbitrary process, internal auditors should follow a risk-based, structured selection method for identifying those applications to review, similar to what was discussed in Chapter 9. A development group, for example, maybe working on applications A, B, and C. Given the relative application risks as well as limited audit time and resources, internal audit may decide to perform preimplementation reviews only for application B. However, if significant postimplementation problems appear in C, management might later second-guess internal audit and ask why system C had not been selected for review. An internal auditor with a consistent selection approach will be able to justify the decision to review B rather than C.
- **Determining the proper auditor's role.** As discussed, when an application has been selected for preimplementation review, internal audit can all too often become overly involved in its systems development and implementation processes. Particularly for applications based on vendor software or developed with rapidly, new IT projects require extensive user and systems development team efforts, with numerous design review meetings. Internal audit often is to participate in these design review meetings, which may cause an auditor role problem. When actively involved in design review meetings where design compromises may be negotiated, internal audit may find it difficult to comment on these same decisions later as audit points. However, if internal audit is excluded from design meetings, it may have a hard time performing the review. For internal auditors to be effective in reviewing new applications under development, their role needs to be defined carefully.
- **Review objectives can be difficul to define** When auditors inform the IT department that a given application has been selected for preimplementation review and requests supporting documentation, they may receive hundreds of pages of requirements studies, general design review documentation, meeting minutes, and other materials. Internal audit may then be asked to review and comment on this mass of materials. An audit objectives and control procedures approach can help auditors choose the relevant materials to review.

Multiple implementation projects and new technologies present some major challenges to internal audit to perform effective IT application preimplementation reviews. However, whether for new applications developed in-house or installed purchased software, internal audit preimplementation reviews will add value to the internal controls environment in the enterprise. In addition, auditors who have been accused in an old joke as being the ones who "join the battlefield after the action is over to shoot the wounded" can now play a proactive role in the applications development process through preimplementation reviews.

(d) Preimplementation Review Procedures

Many of the same audit procedures used in other reviews should be followed for reviews of new applications under development. All too often, internal auditors argue that applications under development are somehow different. However, as fluid and subject to ongoing developmental change as applications under development are, many of the same control objectives and procedures discussed for IT applications are still appropriate for these reviews. Auditors should tailor their preimplementation reviews along the various phases of a new project's development starting at initial project initiation, to requirements definitions definition, to development and testing, and finally to implementation. These same basic steps apply whether an in-house–developed major application, a vendor software package, or a user-led set of desktop applications. There will only be difference in emphasis depending on the application development approach.

When internal audit has selected a given application for preimplementation review, an important first step is to review the overall planned audit program with IT management so that there is an understanding of what the internal auditor expects to find as well as the review approach. Some procedures may be tailored to fit a given application, but the objectives discussed in the next subsections should apply for most preimplementation reviews.

(i) APPLICATION REQUIREMENTS DEFINITION OBJECTIVES When possible, internal audit should get involved in a preimplementation review early in the development phase. Here, internal audit should review the detailed requirements study to determine the overall control status of the new application. If internal audit can identify control concerns during this phase of the applications development, it will be relatively easy for system designers to address and correct them.

Exhibit 19.10 is a set of audit procedures for the requirements definition phase of any project. Internal audit should look for similar requirements no matter how the new application is developed. Some of these procedures, of course, may require modification if the application under review is composed of specialized technologies or it will be a major modification to an existing system. However, internal audit should perform control procedures necessary to satisfy all of the control objectives listed here.

Internal audit may need to decide if any special skills are required to complete the review. If the application involves the use of new or unique systems technologies and specialized supporting software, internal audit may want training on the software product to be used—such as through classes offered by the vendor to the development staff—or it may bring in someone with specialized skills or training. For example, with some large projects that take years to develop and implement,

EXHIBIT 19.10 Preimplementation Review Requirements Definition Checklist

	Audit Step	Reference
1	Obtain a general understanding of the IT department's system development methodology (SDM) standards for both developing new applications and installing purchased software to assure an appropriate requirements definition study.	_____
2	Obtain user-approved request documentation authorizing the detailed application development or purchase.	_____
3	Review the detailed project plan for new applications and ascertain, through discussions with IT and requesting users, that estimates of time and resources seem reasonable and achievable.	_____
4	Check that there was an appropriate analysis, including cost and timing considerations, to determine whether the application should be built in-house or purchased/leased.	_____
5	Determine if any special skills are needed to review application internal controls, such as RFID wireless connections or an understanding of ERP databases. If appropriate, arrange for internal audit staff members to learn new skills through seminars and the like.	_____
6	Identify and review significant internal controls surrounding the new application. Discuss controls with both key users and IT to develop testing procedures.	_____
7	If significant portions of the application involve in-house–developed modules, assess whether appropriate consideration is given to purchased software alternatives.	_____
8	Assess whether the impact of manual aspects of the application have been given proper consideration as part of the requirements definition, such as training needs or process changes.	_____
9	If the application appears to be a candidate for CAATT procedures, begin preliminary audit planning for installation.	_____
10	Review the extent of user sign-offs on the requirements study; based on selected interviews, assess whether users understand the new application and its ramifications.	_____

it can be effective to add a specialist to the staff to cover just their reviews. At the completion of this phase, internal audit might write an informal audit report outlining any preliminary observations and concerns. In addition, workpapers should be started to document the new application control's procedures.

(ii) DETAILED DESIGN AND PROGRAM DEVELOPMENT OBJECTIVES This is typically the longest phase of a new applications project, and internal audit may want to schedule several reviews during this phase. While each of the periodic reviews probably should focus on a specific area of the new application development project, the overall purpose should be to satisfy some of these questions:

- Does the detailed design comply with the objectives of the general requirements definition?
- Do users understand the controls and objectives of the new application under development?
- Has proper consideration been given to application controls and security?

- Is the application being developed according to the IT department's own systems development standards?
- Is the application development process supported by a well-organized project plan, similar to internal audit planning discussed in Chapter 15?
- Have any earlier audit recommendations been incorporated into the detailed design?

During this phase, care should be taken not to become buried in detail. Some IT enterprises may attempt to use internal audit as a quality assurance function for the project. However, overall audit effectiveness will be diminished if internal audit's time is spent reviewing such things as compliance with detailed programming standards.

Reviews of this nature should be limited to periodic testing. Any control-related concerns encountered should be brought to the attention of management so that corrective action can be taken in a timely manner. If the new application is purchased software, often there will be limited in-house design and programming requirements. However, the IT enterprise may have to build file-conversion programs or interfaces with existing systems or table files or report generator definitions. These can represent major efforts, and internal audit still should review controls over the purchased software before it is installed and implemented.

(iii) APPLICATIONS TESTING AND IMPLEMENTATION OBJECTIVES This phase includes testing of the new application, completion of documentation, user training, and conversion of data files. Internal audit often will be able to see if system controls appear to be working as expected and will want to test any embedded audit modules incorporated into the application. Exhibit 19.11 is a preimplementation review application testing checklist for this phase to help internal audit recommend whether the new application is ready for final implementation. Significant system control problems, coupled with management pressures to implement the application as soon as possible, can make this phase difficult. IT often promises to correct control problems in the new application during a "phase two." Auditors often find that because of other priorities, this promised phase two never seems to occur. Internal audit should consider the severity of such control problems and either document them for follow-up review or inform management of the need for corrective action during the current implementation.

At the conclusion of the applications testing and implementation phase, the responsible auditor should prepare a final report that documents significant control issues identified by internal audit and subsequently corrected by the IT development function. This report should also outline any outstanding control recommendations that have not been implemented. While reports up to this point have been informal, this final report should follow normal audit department reporting standards as discussed in Chapter 17.

(iv) POSTIMPLEMENTATION REVIEW OBJECTIVES AND REPORTS Although the new application is no longer in development, this phase of a preimplementation audit is still important. The postimplementation review should take place shortly after a new application has been implemented and has had time to settle down. In other words, internal audit should perform the review after the users have had an opportunity to understand the application and information systems have had time to resolve any

EXHIBIT 19.11 Preimplementation Review Application Testing Checklist

	Audit Preimplementation Step	Auditor Initial
1	Determine if a formal test plan exists, including an outline by key application modules detailing expected data conditions, business rules tested, type of test, and expected results for each module condition tested.	_____
2	Review the results of several recent unit tests to determine if results have been mapped to the test plan, exceptions have been researched, and errors corrected as appropriate.	_____
3	Determine if the application being tested satisfies the original application design requirements; if exceptions exist, determine whether they are properly documented, reviewed, and approved by key users.	_____
4	Interview representative key users to understand their participation in the testing process; where participation appears to be lacking, discuss and document the need for user participation to ensure successful implementations.	_____
5	Review the extent of overall system testing, including key interfaces with other applications and outside service providers.	_____
6	If the completed application does not meet any original requirements, assess procedures in place to determine whether to add procedures later or to allow for discrepancies.	_____
7	If appropriate, initiate a series of internal audit–developed test transactions that emphasize key controls, defined in earlier review steps; review the test results and assess application performance.	_____
8	Summarize the results of application testing activities, and make an internal audit recommendation for the appropriateness of the application implementation.	_____

final implementation difficulties. The postimplementation review determines if application design objectives have been met and if established applications controls are working. It should also look at project controls to determine if the application was completed within budget. Ideally, this review should be performed by another member of the audit staff to provide an independent assessment of the new application.

Many internal audit departments have a fairly formal procedure for issuing audit reports. Draft reports are prepared, auditees prepare their responses after some discussion and negotiation on the draft, and a final audit report is issued, with copies distributed to various levels of management (see Chapter 17). This audit report format is sometimes inappropriate for reviews of new applications under development. An individual internal controls problem with a particular program or output report identified by an auditor when performing a preimplementation review can be corrected by the applications developer almost at once. There is little need to discuss such a finding in the format of a formal audit report draft. The control concern should have been corrected long before the audit report was issued. Both audit and general management, which might expect the more formal audit report with its findings and recommendations, should understand the special report format used for preimplementation reviews.

Informal, memo-type reports should be issued after each phase of the preimplementation reviews. These memo reports should discuss the scope of review activities

and document any audit concerns. If some of the prior concerns have been corrected, the actions taken and current status of the controls issue should be discussed. Of course, internal audit should also develop workpaper documentation covering these review activities, which will serve both to document preimplementation activities and to provide a basis for later applications reviews.

At the conclusion of the preimplementation review, internal audit should issue a formal audit report following audit department standards and report formats discussed in Chapter 17. Where appropriate, this report can discuss preimplementation audit findings and corrective actions taken. However, the main function of this final report is to highlight outstanding control issues that still need to be corrected within the new applications system.

19.7 Importance of Reviewing IT Application Controls

Internal auditors should place a major emphasis on reviewing the supporting IT applications when performing reviews in other areas of the enterprise. Even though good general or interdependent IT control procedures often may be in place, individual applications controls may not all be that strong. An enterprise's applications may have been developed through a series of compromises among users or without any level of proper quality assurance. To evaluate IT applications controls properly, internal audit needs a good understanding of both IT procedures and the specific control and procedural characteristics of each application area.

The effective internal auditor should spend a substantial amount of audit effort reviewing and testing controls over specific IT applications as well as new applications in the development process. Such reviews will provide assurance to general management that applications are operating properly, and to IT management that their design and controls standards are being followed, allowing them to place greater reliance on the output results of such applications. An understanding of application control reviews should be a key component in the modern internal auditor's CBOK tool kit.

Notes

1. Developed in the 1960s, the computer programming language COBOL (*CO*mmon *B*usiness *O*riented *L*anguage) is still used today as a key programming language for older systems on many computers.
2. A common name at the time, K is the mathematical symbol for the number 1000, so Y2K is shorthand for the year 2000.
3. Numerous textbooks and references describe object-oriented programming. A search engine such as Google will provide many further references.

CHAPTER 20

Cybersecurity and Privacy Controls

In our world today of Web-dominated systems and communications as well as networked and wireless communications, security and privacy controls over data and information have become increasingly important. While we cannot forget traditional paper-based manual processes, most internal auditor concerns now are focused on information technology (IT) systems and processes, with emphasis on an area we are calling cybersecurity, an expression that is based on an early name for highly automated processes: cybernetics. The security and privacy controls over these IT processes are a very important area of internal audit control concerns.

This chapter discusses internal audit cybersecurity and privacy controls from two broad perspectives. First, we focus on some of the many cybersecurity and privacy concerns that internal auditors should consider in their reviews of IT-based systems and processes. We have limited our focus to only a selected set of these process areas because the field of IT security controls is vast and sometimes requires technical knowledge beyond the skills of most internal auditors. Nevertheless, all internal auditors should have a general understanding of internal controls procedures here and their associated risks.

Our second cybersecurity and privacy controls focus area includes internal audit's internal procedures. Following the old, "the shoemaker's children have no shoes" admonition, internal audit functions sometimes fail to implement appropriate security and privacy protection controls over their own internal audit processes. This security lapse includes inadequate controls over audit evidence materials, unsecured internal audit workpapers, failure to manage internal auditor laptop computer resources, and many others. While every internal audit department is different, this chapter suggests some best practices for an internal audit function.

The chapter concludes with a discussion of the payment card industry data security standard (PCI-DSS), a guideline that has been developed by major credit card companies, such as Visa and American Express, to help enterprises that process card payments prevent credit card fraud and to provide some protection from various credit security vulnerabilities and threats. Because credit cards are so pervasive, today an enterprise processing, storing, or transmitting payment card data must be PCI-DSS compliant or risk losing its ability to process credit card payments. Internal auditors should understand the high-level key elements of this standard and incorporate it in their reviews where appropriate.

Because there is a great level of complexity to IT cybersecurity practices, many internal audit functions may not have sufficient technical expertise in these areas. However, even though they may not be cybersecurity specialists, all internal auditors should have a high-level common body of knowledge (CBOK) understanding of

cybersecurity risks, high-level controls, and preventive mechanisms. Also, an internal auditor should understand when he or she needs to seek the help and advice of seasoned security experts when performing internal audits.

20.1 IT Network Security Fundamentals

We do not hear too much about major bank robberies today. In the past, when bank vaults carrying large amounts of cash were locked at night but open and protected by guards during the day, it was not uncommon for robbers to arrive at a bank, overpower staff and guards, and depart carrying the cash from the vault. Today, the environment is very different. While a bank may control a huge amount of assets, these assets are only recorded as records on computer files. The potential thief cannot easily stage a holdup and run off with a bag full of those assets. In addition, where the bank does have some cash potentially subject to theft, there are extremely strong controls in place, including recording cameras and the ability to trace currency serial numbers.

Internal auditors should recognize that IT security procedures today are a little closer to those past days of bank vault robberies. It is sometimes easy for a perpetrator to gain access to valuable data records without being detected or without any level of active surveillance. Sometimes the thief can directly download this valuable data without an immediate trace in order to use it for criminal purposes. The IT asset thief may also be taking assets more valuable than just cash, such as credit card authorization numbers that will allow massive purchases elsewhere, passwords to gain access to other even more valuable systems, or even the identities of people to use for further fraudulent transactions.

Lacking proper internal control procedures, an enterprise's IT systems hardware, software, and data face may face any or all four of basic classes of threats:

1. **Interruptions.** A system asset can become lost, unavailable or unusable through the malicious destruction of a program, theft of a hardware component, or improper use of network resources.
2. **Interceptions.** An outside party, such as a person, program, or total computer system, can gain access to an IT asset. An example of this type of threat may be wiretapping to obtain data or the illicit use of program resources. Interceptions can often take place with few traces and can be difficult to detect.
3. **Modification** Here, an unauthorized intruder not only accesses but makes changes to data, programs, or even hardware components. While modifications often can be quickly detected, in some cases they can go on almost unnoticed.
4. **Fabrication.** This threat occurs when an unauthorized person introduces counterfeit objects into an IT environment. These might include spurious transactions to a new work communications system or inserting records in an established database.

These threats were serious in the earlier days of IT systems with their large legacy systems, batch transactions, storage data on mass storage disc drives and tape drives, and limited telecommunications connections. Those same security threats have risen exponentially with today's security threats in our current environment of the Internet, wireless communications, enterprise resource planning (ERP) databases,

and computing devices ranging from sophisticated server systems to small handheld devices. Internal auditors reviewing internal controls in today's environment should be aware of these changes and recognize that threats can be even more significant than in the past.

Just as IT systems have become more sophisticated and better controlled, threats against them have also increased. On a regular basis, we see published accounts of computer security breaches and the theft or destruction of sensitive data. As a single example and certainly not a unique one, just after the end of the holiday shopping season in 2007, the U.S. clothing store retailer TJX Companies announced that someone had hacked into its computer system[1] and made copies of their customer debit and credit card account numbers, addresses, and other identifying data from its 2,000 discount clothing stores, including TJ Maxx. Just as bank robbers in the old days ran off with the stolen cash, never to be found again, the perpetrator who has thousands and thousands of credit card numbers and other personal information can use them in ways that are difficult to trace.

This TJX theft took place over the weeks before and after the holiday shopping season. The data were stolen through the daily transfers of sales data from many of the company's stores. The company, TJX, did not initially detect this breach because the daily sales transmittals from stores over a communications network seemed to have no problems. The perpetrators just made duplicate copies of personal sales data for their own use.

This is an example of one type of computer security breach that occurs worldwide regularly. Many such breaches these involve highly technical exploitations of what might appear to be good internal technical controls. Internal auditors typically do not have the technical skills to assess security risks in many of these IT environments and to make appropriate technical recommendations, but they should have a basic CBOK understanding of computer security concepts for use in a wide range of internal audit reviews.

(a) Security of Data

Enterprise data, whether it is customer account data located in a major data center ERP system database or field data collected on a staff member's laptop, needs to be protected. Although there can be multiple variations and configurations, Exhibit 20.1 illustrates some basic data security concepts. It shows four ways IT data should be protected. Each of these modes is not necessary in all cases, but internal auditors may find it useful to think of data security along these lines.

In some instances, data may require some basic confidentiality protections. As the exhibit illustrates, the control emphasis here is not on confidentiality and integrity threats through the outside protective walls; rather, availability controls are needed to protect programs and data. The extreme example of confidentiality and integrity controls here is the building cornerstone where some key records are sealed in a foundation stone and never seen again while the building is standing. The foundation cornerstone generally does little good in most situations, and the data must be available in a protected, confidential manner. Although there always can be threats, the data should be protected from any unexpected spillage or seepage.

Data integrity is a greater concern. For any data repository, there are always outsiders who try to breach that data protection wall to gain access. In our TJX

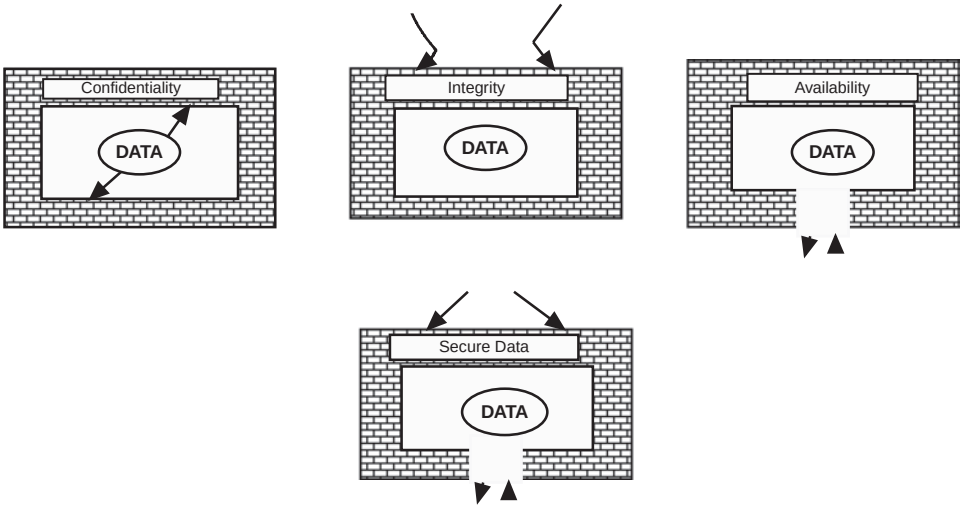


EXHIBIT 20.1 Security of Data Concepts

example, a perpetrator gained access to company data and destroyed its integrity by making unauthorized copies.

While the wall of confidentiality is important, the data generally must become available to others. This is a two-way portal, and the programs and processes controlling the data should make it available only to proper, authorized sources. Password-type controls are very important here and are discussed later in the chapter.

The bottom case in Exhibit 20.1 combines the other three strategies into the concept of a secure data environment. Two other data security concepts are very important here: the concept of firewall and protections against viruses. Both of these are discussed in later sections. Although this exhibit is fairly high level and quite conceptual, internal auditors should think of computer security in terms of these three concepts of confidentiality, integrity, and availability.

(b) Importance of IT Passwords

Passwords are a basic IT control in which a user of a system or data must enter some personal code known only to the user to gain access to the IT resource. Although there can be other more complex configurations, Exhibit 20.2 shows a basic IT password logon exchange. A user enters a password to gain application acceptance, but if the password is incorrect system access is denied.

When reviewing internal controls in an IT application area, an internal auditor should always look for the effective use of passwords. The IT security literature is filled with guidance on the use of passwords. Some best practices in the use of IT passwords are:

- Passwords are a user's responsibility to establish, but administrative rules should be set up to make them hard for others to guess or penetrate. For example, controls and guidance should be in place to prevent the use of employee birthdates or nicknames as passwords.

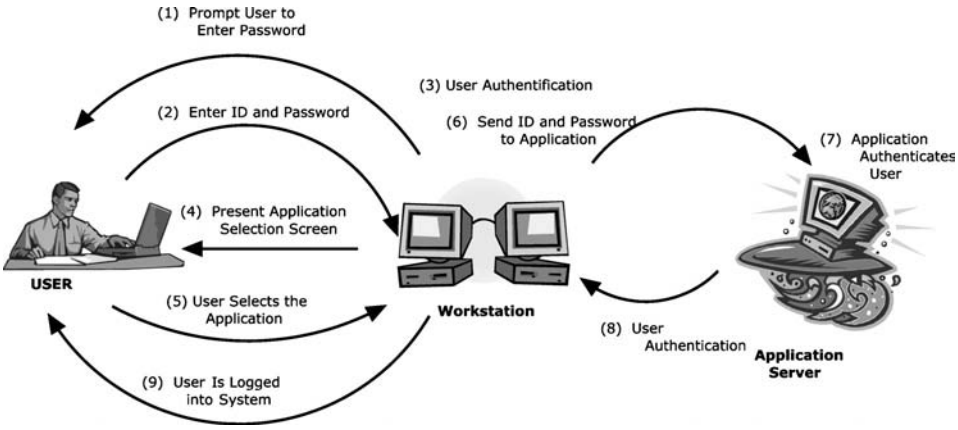


EXHIBIT 20.2 Basic IT Password Logon Exchange

- Passwords should be structured such that they are difficult to guess easily. For example, IT security can set rules requiring a mix of letters and numerals in a password.
- Processes should be in place to require frequent password changes. Sometimes computer operating systems administer this control; if not, procedures should be in place to require regular password changes.
- Processes should be in place to monitor passwords, deny access if perhaps two invalid password attempts, and allow passwords to be reset through an administrative procedure. These processes should allow a user to receive a duplicate if a password has been forgotten.
- Systems should never be installed that generate or require extremely long or complex passwords that typically would be difficult to remember. If too complex, users will post their passwords as a self-help, and the purpose of a confidential password is lost.
- Strong enterprise people-oriented procedures should be in place on the use of passwords. That is, guidance should prohibit the sharing of passwords or posting them in easy-to-see places.

The effective use of passwords is an important IT security authentication control. Other authentication systems exist, such a fingerprint or even eye pupil scanners for some highly sensitive applications, but effective password systems are perhaps the best for regular business applications. Internal auditors should be aware of the requirements for good password controls and should look for effective password systems as part of their many reviews of IT applications internal controls.

(c) Viruses and Malicious Program Code

A computer virus is typically a very small computer program routine that can make a copy of itself and infect another computer without permission or knowledge of the user. The term *virus* is used because it is the kind of program that can attach itself to another system and then spread itself to others as they come in contact with that set of virus code. A virus can spread from one computer to another only when

the virus code is taken to some other uninfected computer, for instance, by a user sending it over a network or the Internet, or by carrying it on a removable medium such as a compact disc or USB drive. Viruses can also spread to other computers by infecting files on a network file system that is accessed by another computer.

Computer viruses first came into the world in the ARPANET, the early 1970s forerunner of today's Internet. Someone—and the identity of the author is subject to speculation—introduced a program on the network that displayed the message "`I'M THE CREEPER: CATCH ME IF YOU CAN`," which began to appear on many system programs.

In the early 1980s days of Apple II and IBM personal computers, viruses reappeared on the floppy disks that were used to share programs and data among computers. Also, although the Creeper message was perhaps cute, virus programs began to become malicious. For example, some of the early viruses just inhabited and took over the memory space of someone's computer, and then were ready to move to another if the infected user tried to solve the problem by sending a floppy disk to another system to seek help. We often forget that these were the days when a popular system such as the Apple II had 32k of memory, and blocking that memory disabled the system.

As time passed, viruses became even more nasty and destructive, and the term *malware* was introduced. Some are Trojan horses, a type of malware named after Greek mythology, that attach to a computer and then sit silently until some date or event is met. Another example is a logic bomb, an unknown program that triggers only when some other event occurs. As an example, a programmer worried about being fired could maliciously insert such a logic bomb routine into the employer's payroll system to delete all systems files if that programmer's ID was ever deleted from payroll records.

Exhibit 20.3 lists some of the more common types of malicious code. There are many other examples of and stories about malware, but the objective of this chapter is not to describe such incidents. The software industry has responded to these malware threats with a variety of commercial products that are constantly monitoring for these types of bad software, and when encountered, either blocking or repairing the bad program code. They are many people around the world who are constantly trying to build a more complex and difficult-to-detect malware routing, and the virus prevention software vendors are working just as fast to catch their code and prevent introductions. This author, for example, has virus protection software loaded on his desktop machine that flashes an Internet message that the antivirus software has been updated sometimes once or twice daily.

EXHIBIT 20.3 Types of Malicious Program Code

Code Type	Characteristics
Virus	Attaches itself to programs and propagates copies of itself to other programs
Trojan horse	Contains unexpected functionality that later performs a disguised function
Logic bomb	Program that triggers only when some other specified event occurs
Time bomb	Program that triggers only when some other specified time period is met
Trapdoor	Undocumented software entry point that circumvents system protections
Worm	Propagates copies of itself through a network
Rabbit	Software code that replicates itself without limit to exhaust the resource

Internal auditors should recognize that software viruses are a constant threat and look for the effective implementation of antivirus software for every computer system reviewed, whether a corporate-level central IT system or a business laptop. An internal auditor should determine that a current version of the software protection software is installed, that it is regularly updated, and that actions are taken when viruses are detected. Policies and software controls should be in place to restrict unauthorized software from being introduced into IT systems operations, whether attempts to download unauthorized programs from the Internet or diskettes and CDs that employees want to load on their home laptops.

(d) Phishing and Other Identity Threats

The growth of online shopping and banking has caused increasingly widespread cybersecurity risks today. Financial motivations have led to an explosion of tactics designed to trick users into divulging their usernames, passwords, and other confidential information, which can then be used to commit a wide range of crimes based on identity fraud. A typical goal had been to clean out the victim's bank account. The information also is often used to help perpetrators commit further fraud and gain unauthorized access to networks. New threats appear regularly, and this section looks at a few of the existing ones.

- **Phishing.** The fraud activity known as phishing, a hackers' term, comes from the scam's parallels with people's love of fishing. Here fake e-mails and Web sites are used as bait to capture a victim's confidential information that is being netted as "phish." In phishing attacks, scammers send out authentic-looking e-mails that claim to come from well-known legitimate institutions. The recipient is encouraged to click on a Web site link in the e-mail. In doing so, victims are then taken to a bogus (or "spoofed") site that is virtually indistinguishable from the real thing.

  Even though only a small percentage fall prey to the trick, phishers can make a significant amount of fraudulent money while the bogus site is up and running. The average length of time for a phishing site to remain online is just four days, according to the Anti-Phishing Workgroup (APWG).[2] With the relatively low cost of setting up a Web site and sending out thousands of e-mails, only a relatively few victims are needed to turn phishing into a profitable scheme. There have been many reported phishing attacks. An APWG January 2007 report revealed an increase of 67.4% in phishing attacks over the same month in 2006. This is a cybersecurity risk.
- **Phaxing.** As a related authentication threat, criminals can send faxes to an enterprise's customers asking them to logon to the Internet and requesting them to send back their URL Internet address. This fax-related version of phishing is called called "phaxing."

Criminals frequently look for social engineering ways to dupe a user and steal that user's identity. Effective controls are not necessarily that complex. For example, users should beware of faxes with a URL[3] address in them asking the recipient to contact the sender via the Internet. A very simple control is to always call up the supposed sender, using a number from the phone book, to confirm he or she sent the fax before responding via the Internet. If one fails to respond in that manner,

there is a chance of having one's identity and authentication information stolen or a bank account rifled.

Identify theft schemes are a growing risk. While it is an enterprise's responsibility to educate its user community and warn people to avoid such frauds, internal auditors should be aware of these schemes and provide appropriate warnings when asked.

(e) IT System Firewalls

A firewall is a software tool that filters traffic between a protected or "inside" and less protected or untrusted "outside" environments. It is a specialized type of software that either allows or prevents certain types of transactions. An enterprise needs to install firewalls between its systems network and the outside world through the Internet or other resources. Firewalls monitor traffic, route some to designated network locations, and block others.

Firewalls are often set up as what is called a screening router, a proxy gateway, or a guard. Internal auditors do not need to understand the technical details of the configurations. From an internal audit perspective, firewalls can be used for some of these applications:

- Screening router configuration firewalls might be used in a situation where an enterprise has three local area networks (LANs), one for its corporate offices, one for U.S. operations, and a third for European Union (EU) facilities. Corporate is allowed to send and receive messages to both facility LANs, but perhaps the United States and European Union are allowed to send only certain specified things to corporate and are not allowed full access across the two facility LANs.
- A proxy gateway firewall would be used when an enterprise wants to set up online price lists and product offerings for outsiders, but the firewall should prevent those outsiders from modifying this price and product information or accessing supporting files connected with the product offerings.
- A guard firewall would be used when an enterprise allows its employees to access most areas of the Web but prohibits access to such things as sports scores or online gambling sites.

In addition to just screening or monitoring network addresses and Web addresses, firewalls can also monitor on the specific content in a message or Web page. They can audit this activity and even report on improper access attempts. Firewalls must be configured correctly, and the configuration must be updated regularly for the internal and external environments. Firewalls protect an environment only if they control all access to a network perimeter. For example, if a firewall was set up to control all access to a LAN but if one of the devices on that LAN had a dial-up modem connection, security could be breached. Firewalls are strong security controls but are often the targets for penetrators.

When performing a data security review, an internal auditor should understand the location and nature of installed firewalls. It is important that the firewall configuration provides adequate protection and is updated regularly. In addition, an internal auditor should look for appropriate review and follow-up activity regarding firewall violation reports.

(f) Other Computer Security Issues

IT networks today must deal with many security threats and malicious code. Coping methods include passwords and firewalls, plus elaborate access controls, the need to use encryption when transmitting data, multilevel security in database administration, and many more. From an internal audit perspective, some of the most important computer security issues focus on the need to establish strong management support for the IT security programs in place and for overall stakeholder education programs to impress on everyone IT network security threats and vulnerabilities.

Ongoing IT internal control reviews by internal auditors should include network and cybersecurity control procedures. In many respects, as these issues become more technically complex, risks increase. Internal auditors may not be strong IT security specialists; if necessary, they should request help from the IT security specialists with the enterprise IT organization.

20.2 IT Systems Privacy Concerns

Privacy is the expectation that confidential personal information disclosed in a private place will not be revealed to third parties, when that disclosure would cause either embarrassment or emotional distress to a person of reasonable sensitivities. *Information* should be interpreted broadly to include images (e.g., photographs, videotapes) and disparaging opinions. It certainly covers all aspects of IT systems and networks.

In our complex networks of Internet-connected systems and ever-advancing technologies, privacy issues on many levels are growing concerns. There is an evolving set of issues here about how much personal data and information individuals should allow to be given to interested enterprises, government authorities, and even other individuals. Similarly, from a privacy and security perspective, an enterprise wants adequate levels of protection. Chapter 26 talks about two U.S.-based laws as examples, the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach Bliley Act (GLBA) that establish some privacy-based rules that internal auditors should be aware of. Other IT-related privacy issues should be on an internal auditor's radar screen. In some instances, these are just evolving issues, but internal auditors should at least be aware of them as they perform internal controls reviews, particularly in IT networks-related area. The next sections describe some evolving privacy issues in today's world of network cybersecurity concerns.

(a) Data Profiling Privacy Issues

As part of everyday life, data are collected from individuals and enterprises, frequently without their consent and often without their knowledge. For individuals, data are collected and stored in a computer system where:

- Bills paid are with credit cards leave a data trail consisting of the purchase amount, type, date, and time.
- The use of supermarket discount cards creates a comprehensive database of all purchases.
- Data are collected when a car, equipped with a radio transponder, passes through an electronic toll booth. The owner's account is debited and a record is created of the location, date, time, and account identification.

- We leave a significant data trail when we surf the Internet and visit Web sites.
- Data are collected when we subscribe to a magazine, sign up for a book club, join a professional association, fill out a warranty card, give money to charities, donate to a political candidate, tithe to a religious organization, invest in mutual funds, make a telephone call, and interact with a government agency. With all of these transactions, we leave a data trail that is stored in some computer file.

Although we have not yet reached the point where the contents of all these many databases are combined, we have come close. In the aftermath of the 9/11 terrorist attacks, U.S. government and law enforcement authorities proposed the development of an airline traveler screening program that would compile data from many consumer data files. That proposal was highly controversial and was not implemented, but a limited version may be developed in future years.

The legal protections for privacy in the United States are weak, and the unfettered collection of data from numerous sources, in an environment where there are few legal restrictions on how the data can be used and merged, can violate privacy and trample on civil liberties. There are few restrictions in the United States on how data can be collected and merged, although stronger laws exist in EU countries, Canada, New Zealand, and Australia. Internal auditors should have a general understanding of these issues.

(b) Online Privacy and E-Commerce Issues

As mentioned, Internet privacy threats are commonplace. We must recognize that the Internet was originally designed as an inherently *insecure* communications vehicle. Hackers often demonstrate that they can penetrate the most secure facilities of military and financial institutions. In addition, enterprises have designed numerous ways to track Web users as they travel and shop throughout Internet sites using a cybersnooping tool called a cookie. Identity thieves are able to shop online anonymously using the credit identities of others, and Web-based information brokers can sell sensitive personal data, including Social Security numbers, relatively cheaply.

There has been extensive media coverage of these issues with a growing public awareness of online privacy issues. Some form of a U.S. Internet privacy law may be passed in the coming years that will provide strong consumer protections in this area, and internal auditors should be aware of these changing rules. While our comments are speculative, such legislation could mandate that every commercial Web site has a privacy policy and require that commercial Web sites clearly explain their data collection practices and provide meaningful methods for visitors to prevent their personal data from being captured and sold to other enterprises.

Internal auditors should be aware of any evolving issues here. Knowledgeable individuals can take steps to prevent their Web-surfing practices from being captured by the Web sites they visit. But, realistically, few people have the requisite knowledge or patience to take advantage of such privacy-enhancing strategies.

(c) Radio Frequency Identification

When consumers wave their keychains in front of the gasoline pump's meter to pay for the fuel just pumped, they are likely to be using radio frequency identification

(RFID) technology. Attached to the keychain is a card that contains a small data chip and antenna called an radio frequency ID access device. RFID technology is frequently used for building-access cards (i.e., ID cards that enable individuals to gain entry into a building or into an office area within a building). Many employee identification cards use RFID technology. These are often called contactless ID cards, because users need only wave the card within a few inches of the reader in order to gain entry.

In the applications just described, the individual is well aware of each and every time the RFID tag is accessed. But RFID tags are tiny and can be embedded in items in ways that are virtually invisible. And reading devices can also be invisible. In the future, RFID readers could possibly be embedded in streetlight poles, and an RFID tag associated with the individual—perhaps embedded in one's driver's license—would record the transactions that person engages in as each day progresses: buying a newspaper at the corner vending machine, entering a supermarket and purchasing groceries, using public transit, entering the workplace, and so on. If RFID tags were embedded in driver's licenses—which most people carry with them at all times—location privacy and anonymity could be things of the past.

Could such a scenario actually happen? Many people find it hard to imagine that we would allow such uses of RFID to occur. However, this is an example of the types of evolving concerns that internal auditors might confront. The challenge for internal auditors is that auditee management and their staffs may have different expectations. There should be a high level of concern regarding some of the RFID privacy issues highlighted throughout this chapter.

(d) Absence of U.S. Federal Privacy Protection Laws

Citizens of most developed countries throughout the world enjoy rights to privacy through laws that are called data protection acts. In most such nations, comprehensive, or omnibus, data protection laws govern how personal information can be used by government agencies as well as commercial-sector entities. Under most such laws, the use of personal information is usually an opt-in or opt-out personal decision. In other words, an individual's personal information cannot be used, say, for marketing unless that person gives affirmative consent.

The United States has no such law, but there are laws covering specific industry sectors, such as the Telephone Consumer Protection Act (telemarketing), the Fair Credit Reporting Act (credit reports and employment background checks), the previously discussed HIPAA (medical records privacy), and other financial privacy rules. Gaps here leave many uses of personal information unprotected. For example, the junk mail one often receives when subscribing to magazines is not covered by a specific law.

The privacy approach taken in the United States is referred to as an opt-out right. For example, consumers' personal information is used to send them unsolicited ads until and unless the consumers sign up to stop these mailings through the direct marketing industry's Mail Preference Service (MPS).[4] Even signing up does not guarantee that your mailbox will be junk free. The MPS is a voluntary standard. Although members of the Direct Marketing Association must subscribe to the MPS as a condition of membership, not all companies that market to individuals are members. Most internal auditors need only to witness the spam in their e-mail in-boxes.

20.3 Auditing IT Security and Privacy

Internal audit should consider performing reviews of IT or cybersecurity controls as well as compliance with established privacy procedures. As discussed, though, this overall area of network security can be very complex and technical, and we would not recommend that typical internal auditors, with limited specialized technical training, initiate a detailed, technical cybersecurity review. Of course, if an overall internal audit function has such technical skills, it can assist in planning and performing such a technical audit.

Many internal audit functions, however, may not have the staff resources to perform a credible, deep technical review in these areas. However, this chapter covers some of the risks and internal control issues that an internal auditor, with only general knowledge of the area and a good understanding of the associated risks, can review effectively.

The use and implementation of IT firewalls is a good example of an effective internal audit review area. We have discussed the types or configurations of IT firewalls that can be implemented. In many instances, however, internal auditors do not need to know, for example, the technical attributes of a proxy firewall. Rather, effective internal auditors should ask some general but very control-specific questions that will enable them auditor to make a high-level cybersecurity review.

As an example, let us assume that an internal auditor is reviewing cybersecurity controls covering the LAN at a small operating division. The internal auditor might ask questions like these:

- Can you give me a diagram of your IT network here showing all internal and external connections within the network?
- Have you installed firewalls for the network and do they protect all access points?
- Is there any way that devices on the network can communicate to other devices, such as a dial-up line through a modem, and bypass the firewall barrier?
- What types of actions or transactions does the firewall screen for?
- Are firewall parameters regularly updated? When was the last update?
- What types of improper access attempts are monitored through the firewall?
- What types of corrective action procedures are in place for attempted firewall violations?
- Can I review some recent firewall violation documentation?

None of these questions really requires an internal auditor to have any strong technical knowledge. Rather, the internal auditor is recognizing that firewalls are an effective security control and is asking, in a general manner, how they have been installed for a LAN. Of course, an internal auditor always faces the risk of receiving a techno-babble answer from an IT person who wants to impress or resents the internal audit process. In that case, the best solution is to write down the response and follow up later with some technical resource. However, the general responses to these questions might indicate some control strengths and weaknesses in the area reviewed.

Exhibit 20.4 contains some cybersecurity internal control audit procedures, covering the areas discussed here. These procedures do not provide complete coverage of all cybersecurity issues facing an enterprise and do not include some evolving

EXHIBIT 20.4 Cybersecurity Internal Controls Audit Procedures

1. Network configuration security controls
   a. Review network configuration diagrams to determine that connections to other networks and computer systems are minimized.
   b. Determine that connections to the Internet are limited and used only when necessary.
   c. Assess the extent of wireless connections, and determine they are appropriately secured.
   d. Review the extent of dial-up connections in place, and determine they are secured with usage monitored.
2. Network system access controls
   a. Assess the adequacy of physical security controls surrounding prime or main data centers.
   b. Review any remote facilities, such as research lab sites, and determine they are following approved central IT processes.
   c. Review configuration to determine that there are no unattended, unsecure workstations attached to the network.
   d. Assess whether suitable physical protections—including hardware, telecommunications equipment, cables, and wiring—are in place for all data centers.
   e. Review the adequacy of backup provisions for electrical power, communication, and storage.
3. Review the extent and currency of written cybersecurity procedures covering:
   a. Personnel screening for new hires.
   b. Information protection and key document controls.
   c. Password and system access procedures.
   d. Utilization of facilities for business use and restrictions on personal use of system resources.
   e. Disposal of sensitive information.
4. Security prevention countermeasure controls
   a. Review overall password policies to determine that there procedures in place to monitor password violations and to require regular password changes, and monitor violations.
   b. Determine that an effective password reset policy is in place where appropriate measures are taken to identify the true owner before granting new passwords.
   c. Review the location and purpose of all installed firewalls and assess their appropriateness.
   d. Determine that firewall activity is audited and that corrective actions are taken when required.
   e. Review the adequacy of protection procedures in place to prevent sniffing and spoofing.
   f. Assess policies in place for using encryption, and assess whether encryptions procedures are adequate.
5. Security incident monitoring and investigation techniques
   a. Determine that there are formal incident reporting and investigation procedures in place.
   b. Determine that appropriate investigation and action plans are implemented in the event of security breaches.
   c. On a test basis, review actions taken on any reported suspicious events to determine that applicable corrective actions were taken.
   d. Review the skills, training, and documented actions of the established incident response team to assess effectiveness.
   e. Determine that there has been adequate coordination with law enforcement agencies to, at a minimum, support cybersecurity issues.
6. Cybersecurity training
   a. Determine that all affected staff members are trained in cybersecurity risks and issues, as appropriate.
   b. Look for a program of enterprise-wide security training to raise awareness and highlight potential risks.

privacy issues. Internal auditors should develop a high-level understanding of the risks and controls in these important areas. As we become a highly networked and interconnected world, enterprises need to build and establish strong and effective cybersecurity controls. An internal auditor may not be a technical guru here, but a general understanding of risks and control issues in these areas will help make him or her a more effective aid to enterprise management.

20.4 Security and Privacy in the Internal Audit Department

Internal auditors as an operating function in the enterprise and as individual internal auditors need to establish their own security and privacy procedures and best practices. Internal auditors regularly visit a site and capture information and data, either in a hard- or soft-copy format, covering the area of their review as well as other information from the site audited. Depending on the nature of a review, that captured audit evidence material must be maintained in a secure and confidential manner.

Most, if not all, internal audit functions today have moved from the days of pencil-and-paper workpaper records and voluminous supporting records to laptop computers and the use of extensive automated processes. In past years, internal auditors kept their work in thick workpaper binders, and after an individual audit was completed, the approved workpapers were filed in a fairly secure audit department library. There was always a risk that a workpaper binder could become lost, but today's laptop era may present greater internal audit privacy and security risks.

(a) Security and Control for Auditor Computers

Once considered an advanced audit technique, laptop or desktop computers use by internal auditors is essentially a standard today. Based on Microsoft or Apple operating system software, these machines are used for writing audit narratives and the audit report findings with word processing software, preparing analyses and other schedules with spreadsheet software, communicating with others on the audit team as well as the Web through e-mail and the Internet, and many other tasks.

Internal auditors carry their laptops with them, work on them while on flights to audit assignments, and take them to auditee sites. While an auditor's laptop may carry critical files and information at any one time, the machine also has some intrinsic value. Carried through airport lounges or tossed into the backseat of rental cars, laptops are subject to theft. While there is some cost associated with the laptop itself, the major cost of any laptop system loss is the internal audit data contained in the system's files. Some important techniques for protecting auditor laptops include:

- **Auditor personal responsibility for auditor laptops.** Through training, audit department standards, and just good guidance, all internal auditors who have been assigned a laptop should be reminded that they have a strong responsibility for the security of their system. This type of standard can include such simple guidance as to always keep one's laptop in the locked trunk of the automobile rather than in the back seat, not to leave it sitting unattended, and not to allow family members to use it such that files could be erased or corrupted.
- **File backup procedures.** Whether using a backup site at the headquarters internal audit office or a special USB clip or device, auditor laptop computers

should be regularly backed up. Storage devices—particularly USB devices—are now very cheap, and software tools for backups are readily available today. Procedures should be established for internal auditors to perform a 100% daily backup of their systems. There is no need to keep multiple versions here, because the current backup copy is usually sufficient,

- **Physical locks and mechanisms.** Numerous small devices similar to cable bicycle locks can connect a laptop to a desk or some other-difficult-to move object. These devices are relatively inexpensive, and an internal audit function should adopt them for internal auditor use.
- **Antivirus and other tools.** This chapter has discussed computer malware and the need for antivirus protection. The same types of software tools should be installed in all internal auditor laptops.

An internal auditor's laptop computer is often a repository for auditor narratives, copies of documents, and other key audit evidence. Good security procedures should be established to protect these important internal audit resources. Even when an internal audit function does not use laptops and relies on desktop machines, similar auditor security practices should be installed.

(b) Workpaper Security

Workpapers are the key documents that carry auditor evidence and the results of the internal audit assignment work. Chapter 16 talks about good workpaper documentation procedures, and audit department security over those workpapers is very important. Sarbanes-Oxley rules discussed in Chapter 4 require that, as audit evidence, workpaper files should be retained for a seven-year period. Also, in a litigation situation, internal audit workpapers can become legal evidence in civil or even criminal court proceedings.

In today's environment, workpaper documentation can be a combination of soft-copy computer files and hard-copy documents. Internal audit needs strong procedures to catalog, store, and secure their internal audit workpapers. Just as a book in a public library has a catalog number to allow its easy retrieval, an internal audit function should develop some kind of numbering scheme for cataloging its workpapers. There is no one best approach here, but in launching such a program, the chief audit executive (CAE) should realize that seven years is a long time and that there can be many changes in the enterprise and its operating units.

Just as a major purpose of the library book numbering process is to allow people to check out a book for their use, audit workpapers should be organized in such a manner that a workpaper binder can be checked out for use. This use should be limited to other members of the internal audit staff and external auditors on request. Tracking records should be maintained to identify the location of any checked out workpapers at any time.

Workpaper security is always a concern, and whether the files are in hard- or soft-copy format, procedures should be established to back up and protect them. Hard-copy documents should be kept in a secure, locked facility with limited access. Because a seven-year accumulation can create quite a volume of materials, arrangements should be made to send older workpapers to a secure document repository service. Soft-copy workpaper materials should be backed up as well. There can be a particular concern here, however, as file formats can change. Consider the IT

EXHIBIT 20.5 Internal Audit Workpaper Security Best Practices

- Establish general internal audit department workpaper standards defining best practices for such areas as capturing audit evidence, recording volume bulk evidence materials, and others.
- Develop general procedures for preparing workpapers in hard-copy paper-based formats and/or office systems–based soft copies, and establish guidelines for when each should be used.
- Establish general indexing or numbering systems for all workpapers that identify the unit, type of audit, and year of audit as well as general workpaper cross-referencing guidance.
- For laptop or desktop computer-based soft-copy workpapers:
  - Develop consistent file and file folder naming conventions that identify originators and dates of last changes.
  - Establish read and data update security controls.
  - Backup files to a secure server or other facility at least daily.
  - Establish workpaper update procedures such that when a printed version of a workpaper is updated, the automated version is updated as well.
  - Copy workpapers of completed audits to a secure repository such that data can be accessed later, given seven-year minimum retention requirements.
- For hard-copy, paper-based workpapers:
  - Establish consistent content naming conventions with descriptive names, dates, and auditor initials included on all workpaper sheets.
  - Establish security rules for paper-based workpapers during the audit process to prevent unauthorized persons from accessing workpaper files left on auditor desks, etc.
  - Develop consistent procedures for transporting and shipping workpaper files.
  - Because subsequent content alterations are sometimes difficult to trace, establish strong audit staff standards and guidelines on the improper alteration of workpapers.
  - Place all current workpapers in a secure facility with strong check-in and check-out rules.
  - Make arrangement for all older workpapers to be retained in a bulk storage repository.
- Build a comprehensive database to link all workpapers to the audit, completed report, and significant findings.
- Whether hard or soft copy, establish consistent workpaper review practices to identify the timing of supervisory reviews and nature of any changes.
- On a limited and test basis, perform quality reviews of older audit workpaper files to determine their ongoing accessibility.

formats that were used not so long ago in the days of floppy disk files and earlier versions of word processing software. If needed, files stored in those formats would present problems today. We cannot predict the future here, but if technology changes appear to be making old soft-copy versions hard to use, arrangements should be made to convert them before it is too late.

Exhibit 20.5 lists some internal audit workpaper security best practices. As important documentation describing all internal audit activities, workpaper security is important. It is always necessary to allow other members of the audit team to review older workpapers in order to follow established audit programs or procedures and the like; close attention should be given to preventing any alteration of workpapers once the audit assignment has been completed and the documentation approved. There is always the danger of a rogue member of the internal audit team making

after-the-fact changes to the evidence gathered through audit workpapers, for any of several reasons. These alterations can be prevented through read-only controls installed on soft copy-versions but hard-copy versions may be difficult to protect.

(c) Audit Reports and Privacy

Internal audit reports, as described in Chapter 17, are documents that describe internal audit's activities for a planned audit project, the procedures performed, findings and recommendations, and auditee management's responses to those findings along with their plans for corrective action. By their nature, audit reports are not documents for mass distribution. They should only be shared with auditee management, enterprise senior management, external audit, and the audit committee. Disclaimers should be added to report documents stating that they are not to be copied or shared, and the CAE and members of the audit team should regularly emphasize the confidentiality needs for these documents.

Our comments here on workpapers have emphasized related security issues. Published audit reports raise a privacy issue as well. Comments in the findings section of an audit report can very much damage the professional credibility of portions of the enterprise and members of management. Care should be given to securing and protecting audit reports from access to unauthorized persons.

(d) Internal Audit Security and Privacy Standards and Training

Our comments on internal audit security and privacy procedures represent some best practices that should be considered by internal audit functions, no matter their size, industry, or geographic location. However, while it is one matter for the CAE to agree and install such procedures, all members of internal audit should be aware of these practices on an ongoing basis.

Internal audit should establish departmental standards for workpaper security and privacy. Arrangements for a formal library repository should be established within the enterprise. This would typically be located nearby the CAE and enterprise headquarters; however, for a large, multi-unit enterprise and larger internal audit function, off-site or multiple workpaper library repositories could be established. The locations should be secure with overall administrative control assigned to an administrative staff member. With ongoing seven-year retention requirements, the hard- and soft-copy workpaper repositories and libraries should be organized such that later retrieval will be comparatively easy.

Audit department security and privacy standards should be included in audit department standards and training. In particular, as discussed, every member of the audit team should be asked to recognize the privacy and protection needs of their assigned audit computers. Although internal auditors make security and privacy related recommendations in many audit areas, they also should always remember that these rules are extremely important for internal audit itself as well.

20.5 PCI-DSS Fundamentals

The PCI-DSS data security standard, launched in September 2007 by the Payment Card Industry (PCI) council—a worldwide industry group led by American Express, Discover, MasterCard, Visa, and others—must be used by anyone wanting to accept

EXHIBIT 20.6 PCI-DSS Requirements

1	Build and maintain a secure network.	Install and maintain a firewall configuration to protect cardholder data.
2	Build and maintain a secure network.	Do not use vendor-supplied defaults for system passwords and other security parameters.
3	Protect cardholder data.	Protect stored data, and do not store card and transaction data unnecessarily.
4	Protect cardholder data.	Encrypt transmission of cardholder data and sensitive information across public networks.
5	Maintain a vulnerability management program.	Use and regularly update antivirus software.
6	Maintain a vulnerability management program.	Develop and maintain secure systems and applications.
7	Implement strong access control measures.	Restrict access to data by business need to know.
8	Implement strong access control measures.	Assign a unique ID to each person with computer access.
9	Implement strong access control measures.	Restrict physical access to cardholder data.
10	Regularly monitor and test networks.	Track and monitor all access to network resources and cardholder data.
11	Regularly monitor and test networks.	Regularly test security systems and processes.
12	Maintain an information security policy.	Establish and maintain high-level security principles and procedures.

credit cards as a form of payment. Because credit cards are so pervasive in enterprise commerce and because the failure to comply with this standard can result in a variety of fines and, potentially, the loss of the right of an enterprise to accept credit cards at all, we are providing an overview of this important new cybersecurity standard.[5]

PCI-DSS is a worldwide standard that has been established to comply with a massive number of local and national rules and following guidelines of the major credit card companies. The standard contains configuration and audit guidelines that cover *any* IT device that accepts credit cards as payment. The phrase "any IT device" is quite broad and goes beyond the more standard computer systems. These include the point-of-sale devices found in retail stores, any site accepting e-mail payments, and a wide range of others.

Exhibit 20.6 shows the 12 basic requirements for a PCI-DSS implementation. These requirements are very high level and oriented to the credit card industry. Many deal with good general network security and cover areas already discussed in this chapter, such as installing effective firewalls, the use of antivirus software, and the importance of security policies.

Effective use of these requirements means going a little further in understanding cybersecurity control needs. For example, Requirement 11 in Exhibit 20.6 is the need to test security systems and processes regularly. This might require an enterprise to:

- Test security controls annually
- Run internal and external data scans quarterly

- Perform annual penetration tests on systems and applications
- Use tools for network and host intrusion detection
- Implement file integrity monitoring procedures

Many enterprises worldwide are working to achieve PCI-DSS compliance. It is a hybrid mix of a standard, such as the Institute of Internal Auditors standards of Chapter 8, and regulation, where the rule of law requires compliance. It is also a good example of the growing importance of cybersecurity issues.

Internal auditors working in enterprises that use credit card payment transactions may already be involved with these compliance efforts. If not, they should discuss these potential compliance concerns with financial and IT management within their organizations. The PCI-DSS standard has been instituted by the credit card industry, but in the future, other industries may develop similar standards.

20.6 Internal Audit's Privacy and Cybersecurity Roles

Internal auditors should be aware of the growing and evolving cybersecurity and privacy issues, both in their enterprises and worldwide. As discussed, many of the issues here can become quite technical, but all internal auditors should acquire a general understanding of the areas discussed in this chapter. For example, most laptop computer users today are at least aware of the risks of computer viruses. An internal auditor should go a step further and understand the kinds of controls that can be applied to eliminate such risks and then implement them.

The cybersecurity and privacy risks and issues discussed in this chapter are constantly changing and evolving. Software vendors, for example, will develop a new protection technique for some type of malware virus only to have someone beat or get around the protection almost as soon as it is released. Most internal auditors will not become experts on these highly technical issues, but all internal auditors should have a CBOK understanding of cybersecurity and related IT privacy risks.

Notes

1. Numerous Web accounts have been published of this breach, such as: www.associatedcontent.com/article/128326/tj_maxx_and_marshalls_customers_data.html.
2. A workgroup committed to reducing Internet frauds and scams: www.antiphishing.org/.
3. *URL* is an abbreviation of *U*niform *R*esource *L*ocator, the global address of documents and other resources on the Internet.
4. A service to prohibit unwanted consumer mail at www.dmachoice.org/MPS/proto1.php.
5. More information on the standard can be found in PCI's Web site, www.pcisecuritystandards.org, and in Timothy Virtue, *Payment Card Industry Data Security Standard Handbook* (Hoboken, NJ: John Wiley & Sons, 2008).

CHAPTER 21

Computer-Assisted Audit Tools and Techniques

Internal auditors gather evidence from an enterprise's books and records to support their conclusions. This audit evidence includes the actual paper-based documents as well as data to support that these documents or transactions were properly recorded in a timely manner, and with appropriate authorizing signatures or notations. Today most of those documents are information technology (IT)–based and paperless. Internal auditors are challenged to review and understand those paperless documents and require procedures to support their audit conclusions. While internal auditors test and review the internal controls surrounding those IT systems, they often need tools to better understand and evaluate the completeness and accuracy of the often-large amounts of data stored in the files and databases of the applications. Specialized, audit-oriented IT techniques are often the most efficient way to examine all recorded items on the supporting computer files. Internal auditors can also act with greater independence by developing their own specialized IT file retrievals. These represent some of the many approaches to retrieving data through the use of computer-assisted audit tools and techniques (CAATTs), independent auditor–controlled software to assist in internal audit efforts.

A fundamental requirement of internal audit is to obtain evidence on the validity of accounting and operational data. However, large volumes of data or missing paper documents often makes this review of evidence difficult or almost impossible. This chapter describes internal audit approaches to testing, analyzing, and gathering detailed evidence from data contained on IT applications through the use of CAATTs. These techniques allow an internal auditor to review the contents of IT applications data in files, ranging from accounting systems on large database repositories to smaller systems residing on departmental desktop systems. Although some CAATTs require specialized data processing skills, many can be performed by the typical internal auditor, with no particular programming skills.

There are many tools and techniques available to help make audit reviews of IT-supported systems more efficient and effective. While the operation of some CAATTs requires specialized IT skills and tools, many others can be executed by internal auditors at all levels. All internal auditors should have a basic common body of knowledge (CBOK) understanding of the general use of CAATTs to access and review automated data in support of internal audits. If an internal auditor does not have the skills to execute a particular CAATT process, he or she should have a sufficient CBOK level of knowledge to describe the potential CAATT retrieval needs and request help from a more IT-oriented member of the internal audit team.

21.1 Understanding Computer-Assisted Audit Tools and Techniques

A CAATT is a specialized computer program or process, controlled by internal audit, that is used to test or otherwise analyze data on computer files. Terminologies change over time, and an internal auditor will sometimes see the term *CAAT* or *CAAP* rather than *CAATT*; the first refers to just "techniques" while the second is an abbreviation for "procedure." All of these expressions refer to similar techniques and can be used interchangeably. The American Institute of Certified Public Accountants (AICPA) uses *CAATTs,* the term preferred for this book.

In the early days of data processing systems, auditors typically relied on the printed outputs from IT systems and used conventional audit procedures to read, test, and analyze these computer-generated reports. As IT systems became more pervasive with ever-larger data files, auditors needed better approaches to evaluate the documentation and records stored in the systems. In the early days of IT systems, a few pioneer internal auditors used CAATTs to read and analyze financial data on large computer files.

The necessity for CAATT procedures first became very evident with the Equity Funding fraud in the early 1970s. Equity Funding Corporation, an insurance company, was reporting very significant growth and earnings from the late 1960s through the early 1970s. It was later determined, however, that Equity Funding's growth and earnings were based on a massive management fraud in which fictitious insurance policies were entered on the company's computerized records. At the time, the external auditors relied on the printed report outputs generated by the Equity Funding computer systems rather than on the data recorded on computer files. Had the external auditors looked at the contents of those computer files, they might have detected the fraud. Equity Funding did not have a significant internal audit function, and an Equity Funding employee eventually revealed the fraud.

After the fraud was discovered, many professionals pointed out that it could have been detected much earlier had the auditors analyzed the computer files. A review of IT-generated output reports alone was not sufficient. The auditors needed both to independently review computer procedures and to analyze the contents of computerized records. The Equity Funding fraud launched what was then called computer auditing—now IT auditing—and the use of CAATTs.

A basic CAATT process is an auditor-controlled computer program that can be run against production IT files to analyze and summarize that data and perform other audit tests. Before powerful desktop software tools existed, a CAATT was considered to be an advanced technique. End users typically relied on their data processing departments to write special retrieval programs to give them the various output reports requested. Both internal and external auditors later began to use generalized audit software to develop their own programs independently for testing and analyzing data. This generalized software became the basis for CAATTs. The term *CAATT* is used to define specialized IT systems and procedures to assist internal audit. An example might better clarify the concept of a typical CAATT. Assume that internal audit is interested in testing the accuracy of the account agings from an automated accounts receivable computer system; however, since most calculated data for that system is stored on computer files, there are no significant paper reports describing these calculations. Internal audit is concerned that the receivables, as reported on the aged trial balance report, may not be properly aged as to the number

of days due. Thus the receivables account balances may be over- or understated. Internal audit can test these agings using any of three approaches.

First, internal audit could use traditional, manual approaches, where items are selected from an IT output report and then are traced back to any original source documents that may exist. Internal audit can then determine if the items selected are properly entered on IT system records and if the aging calculations are correct. This will work if paper records are available. However, because of the volume of receivable records in typical IT systems, internal audit can only selectively trace and test these items. Some exception conditions may be missed with such a manual test. In addition, internal audit might not be able to easily determine if the dates of transaction-based agings are functioning correctly.

A second approach is to perform an internal controls review over the automated accounts receivable system. If internal controls over the application are found to be good, internal audit can rely on system output reports. IT application internal controls reviews are discussed in Chapter 19. A review of systems documentation and perhaps of a selected program source code determines whether the system is properly aging receivables. Internal audit would then test those controls by, for example, running some test transaction into the system, through either manual transactions or another CAATT. Properly performed, this review can detect significant internal control problems as well as determine whether the system is generally working in a correct, well-controlled manner. However, internal audit would only be able to estimate the total extent of the financial statement adjustments necessary due to any account aging errors. In conjunction with this test, internal audit must determine that controls over data entry and error correction are adequate.

The third approach is to use a CAATT application to recalculate independently all of the agings in the accounts receivable system, develop totals for the accounts receivable balance, and produce a listing of any unusual exception items. Internal audit might perform this third, CAATT-oriented approach through five steps:

Step 1. Determine CAATT objectives. Internal audit should not just use the computer to test a system without a clear set of starting audit objectives for any CAATT. In the preceding examples, internal audit would have an objective of determining if accounts receivable agings are correctly stated.

Step 2. Understand the supporting IT systems. Internal audit should review IT systems documentation to determine how accounts receivable agings are calculated, where these data are stored in the system, and how items are described in system files.

Step 3. Develop CAATT programs. Using generalized audit software, other retrieval packages, or a computer language processor, internal audit would write its own programs to recalculate accounts receivable agings and to generate totals from accounts receivable files.

Step 4. Test and process the CAATT. After testing the programs, the internal auditor would arrange to have the CAATTs processed against production accounts receivable files.

Step 5. Develop audit conclusions from CAATT results. Similar to any audit test, audit conclusions would be drawn from the results of the CAATT processing, documented in the workpapers, and discussed in the audit report, as appropriate.

This is the general approach to developing and processing CAATTs. It follows the same steps internal audit would use for establishing audit objectives and performing appropriate tests on any system or process. The CAATT can be developed through generalized audit software programs run on the production computer system, specialized software run on the auditor's own laptop computer, or specialized auditor-use-only program code embedded in an otherwise typical production application. CAATTs can enhance internal audit processes in some of these areas:

- **Increase audit coverage.** CAATTs can allow an internal auditor to review and analyze such components as massive financial databases where internal auditors do not have easy access to online screen reports and certainly not paper reports.
- **Focus on risk areas.** Similar to the last point and our example of testing accounts receivable agings, CAATTs often allow an internal auditor to review and investigate areas that have not received a high level of internal audit scrutiny.
- **Increase cost effectiveness.** Although CAATTs may require some incremental time and cost to develop, they can be very effective for analyzing large volumes of IT-resident data over multiple periods.
- **Improve audit credibility.** CAATTs provide internal auditors with the ability to look independently at complex databases and provide detailed analyses and recommendations; that type of analysis can very much improve internal auditor credibility.
- **Improve integration of IT, financial and operational specialty auditors.** CAATTs often are used to analyze financial and operational processes using IT processes. They will enable auditors with financial and operational objectives to talk and coordinate audit objectives and needs better.
- **Encourage auditor independence from IT operations.** Internal auditors do not have to be heavily dependent on the IT systems and infrastructure to operate their CAATTs. Although strong coordination is essential, internal auditors can operate fairly independently.

Internal auditors should have a good understanding of when CAATTs should be used to enhance the audit process, the types of software tools available, and how to use a CAATT in an audit. They are an important type of internal audit tool.

21.2 Determining the Need for CAATTs

CAATTs can enhance both the audit process and internal auditor independence. However, CAATT procedures sometimes can be time consuming to develop and, unless properly planned and designed, will not always be cost effective. Internal audit needs to understand when a CAATT might increase overall audit efficiencies and when it will not. This section discusses areas where CAATTs will enhance an audit and areas to consider when developing and implementing a CAATT. Other sections discuss alternative CAATT approaches and procedures for implementing them as well as some problems with CAATTs.

Before developing a specific CAATT, an internal auditor should first determine if the planned approach is appropriate. All too often, a member of management may have attended a seminar about audit efficiencies and then will ask the internal

audit team to do something to improve audit efficiency by using IT resources as part of internal audits. This was particularly true several years ago, when management expressed strong concerns about all levels of audit costs associated with Sarbanes-Oxley Act Section 404 reviews, as discussed in Chapter 4. This type of improved audit efficiency directive often may result in disappointment for all parties. Similarly, a highly technical internal auditor sometimes may develop a technically interesting CAATT as part of an audit even though it really does not support the overall objectives of that review. The result may be interesting but will not contribute to the overall effectiveness of the internal audit's objectives. The decision to develop and implement a CAATT in support of an internal audit will depend on the nature of the data and production programs being reviewed in the audit, the CAATT tools available to internal audit, and the objectives of the audit. Internal audit needs an overall understanding of CAATT procedures in order to make this decision, and should consider these points:

- **Nature or objectives of the audit.** Internal audit should initially evaluate the materials to be reviewed in a planned audit and consider the size and format of any IT-based audit material data. Audits based on values or attributes of computerized data are typically good candidates for CAATTs. For example, the accounts receivable audit discussed earlier is a good CAATT candidate because there is generally a large volume of transactions but minimal paper records. Many of the operational and financial audit areas discussed throughout this book are also good candidates for CAATTs. However, a business ethics policy audit, as discussed in Chapter 24, requires an examination of published procedures-related records and may not be a good candidate for a CAATT. While a computerized database can summarize the ethics policy data, it provides only indirect support for the prime audit procedures.
- **Nature of the data to be reviewed.** CAATTs are most effective when both data and decision-dependent information are based on automated systems. For example, a manufacturing inventory system will have most of the descriptive information about its inventory on IT system files. Inventory-related data is input directly, and inventory status information is based on system reports on output screens. There are often only limited paper-based original records. Internal audit procedures for inventory here might include an analysis of manufacturing costs, and inventory system attributes can be summarized and analyzed through a CAATT. Other computer systems are comprised of little more than log files that organize otherwise manual records. An engineering project authorization system might have summary data stored on a systems file, but most of the information about the projects may be on manual, paper-based files. CAATTs might not be too effective in these areas because internal audit also would need to review the manual data. Audits in areas where there is heavy dependence on IT data are good potential candidates for a CAATT.
- **Available CAATT tools and audit skills.** Internal audit must develop its CAATTs using the automation tools available within the audit department or IT function. If internal audit does not have or has not budgeted for specialized CAATT software, an internal auditor cannot develop CAATTs that require such software. Internal audit needs to consider the types of audit software available before embarking on any CAATT projects. That availability may be based on both audit budget constraints and product limitations.

- **Auditor skills.** Although training materials are available, internal auditors can learn many processes on their own. When IT technical problems occur, the in-charge auditor must assess whether technical audit specialists are needed and are available for the CAATT-development project.

These points are stated in very general terms, but they are areas to be considered when planning the overall strategy for using CAATTs.

These comments point to many other areas where a CAATT will be difficult or not particularly cost effective. However, internal audit should keep an open mind and always consider using CAATTs to enhance internal audit effectiveness. Given the lack of paper-based audit trails in many of today's automated systems, an internal auditor has little choice but to use computer-assisted audit procedures. The challenge to internal audit is to identify appropriate areas for CAATTs.

Computer technology has changed extensively over the years. The batch-oriented IT systems of not too many years ago have been replaced by online, database-oriented applications. Large centralized computer installations have been replaced, in many environments, by networked client-server workstations. Despite these changes, however, the auditor's basic approach for defining CAATTs has not really changed. For example, in 1979 the AICPA published an audit guide, *Computer-Assisted Audit Techniques,*[1] which provided some basic direction on the use of CAATTs. Although now long out of date and out of print, it contained a good list of the types of audit procedures that can be performed through the use of CAATTs. This set of procedures, adapted for internal auditors, emphasize:

- **Examining records based on criteria specifie by internal audit.** Because the records in a manual system are visible, internal audit can scan for inconsistencies or inaccuracies without difficulty. For records on computer data files, internal audit can specify audit software instructions to scan and print records that are exceptions to the criteria, so that follow-up actions can be taken. Examples of specified areas are:
  - Accounts receivable balances for amounts over the credit limit
  - Inventory quantities for negative and unreasonably large balances
  - Payroll files for terminated employees
  - Bank demand deposit files for unusually large deposits or withdrawals
- **Testing calculations and making computations.** Internal audit can use software to perform quantitative analyses to evaluate the reasonableness of auditee representations. Such analyses might be for:
  - Extensions of inventory items
  - Depreciation amounts
  - Accuracy of sales discounts
  - Interest calculations
  - Employees' net pay computations
- **Comparing data on separate files** When records on separate files should contain compatible information, software can determine if the information agrees. Comparisons could be:
  - Changes in accounts receivable balances between two dates, comparing the details of sales and cash receipts on transaction files
  - Payroll details with personnel files
  - Current and prior-period inventory files to assist in reviewing for obsolete or slow-moving items

- **Selecting and printing audit samples.** Multiple criteria may be used for selection, such as a judgmental sample of high-dollar and old items and a random sample of all other items, which can be printed in the auditor's workpaper format or on special confirmation forms. Examples are:
  - Accounts receivables balances for confirmations
  - Inventory items for observations
  - Fixed-asset additions for vouching
  - Paid voucher records for review of expenses
  - Vendor records for accounts payable confirmations
- **Summarizing and resequencing data and performing analyses.** Audit software can reformat and aggregate data in a variety of ways to simulate processing or to determine the reasonableness of output results. Examples are:
  - Totaling transactions on an account file
  - Testing accounts receivables aging
  - Preparing general ledger trial balances
  - Summarizing inventory turnover statistics for obsolescence analysis
  - Resequencing inventory items by location to facilitate physical observations
- **Comparing data obtained through other audit procedures with IT system data files** Audit evidence gathered manually can be converted to a machine-readable form and compared to other data files. Examples are:
  - Inventory test counts with perpetual records
  - Creditor statements with accounts payable files

Although these techniques were originally developed for external auditors and date before the days of integrated database files, they techniques are generally still applicable for internal auditors. The number and sophistication of these CAATTs increase as an individual internal auditor becomes more experienced in their use.

21.3 CAATT Software Tools

In the early days of computer systems, IT users had to submit a request to the programming department for any type of special report or analysis program. Writing computer programs was often a difficult and time-consuming process performed by specialists in the IT department. Internal auditors were often suspicious of that approach. Just as an auditor who was interested in the account balance for some population of manual records would not ask the auditee for the balance but would examine the records to calculate an auditor-developed total, auditors often preferred to use their own programs controlled by internal audit to analyze computer-based data. This led to the development of what has been called generalized audit software with its several common categories or types of computer audit software:

- Generalized audit software products
- Report generator languages
- Test data techniques
- Specialized audit test and analysis software
- Expert systems and inference-based software
- Embedded audit procedures

Depending on the overall IT environment and internal audit's objectives, one or more of these CAATTs may be used in a given audit situation. Some require specialized technical skills, but most can be implemented by the generalist internal auditor. To be effective, any internal audit department operating in today's highly computerized environments should use some type of audit software.

(a) Types of CAATTs: Generalized Audit Software

In the early days of IT auditing, most business applications were written in older programming languages, such as COBOL. Auditors of the time usually had neither the technical skills nor the time required to write their own retrieval programs to independently access data. When an internal auditor wanted to test or review the contents of a large data file based on a COBOL program, it was usually necessary to submit a request to what was then called the data processing department to produce that report. The auditor would be dependent on some programmer to produce the requested report and could not fully act independently. The major public accounting firms solved this problem of lack of auditor independence in the early 1970s by developing simple audit retrieval programs. In addition to convenient data retrieval capabilities, this software often contained other common audit functions, such as sequence number gap detection and audit sampling procedures.

This software eventually was marketed as generalized audit software (GAS). It was originally mainframe or legacy system based, although several good products are suitable for laptop computers today. GAS offers internal auditors some of these advantages:

- **Increased independence from information systems.** GAS allows internal audit to perform tests of an application without asking the IT function to write the necessary retrieval software, giving auditors an extra level of independence.
- **Increased audit efficiencies** GAS software can perform such routine actions as confirming accounts receivable records and producing confirmation letters more efficiently than traditional audit procedures. In addition, such a CAATT will almost certainly be used over multiple years, so its development costs can be spread over time.
- **Opportunity to observe other controls.** By using an independent set of programs on the auditee's systems operations, internal audit can observe and develop a better understanding of other IT controls. For example, internal audit may observe procedural weaknesses in work schedules or tape cartridge retrievals from the data center library. While not related to the planned tests of given data files, these observations often can point to areas for subsequent audit work.

Exhibit 21.1 outlines the typical development steps for planning and building a CAATT. It shows this generalized software program code as batch transactions much more easily constructed than a conventional program written in a language such as Visual Basic or SQL. This type of programming code is usually easy to learn. Generalized audit software was introduced in the mainframe computer era, when few easy-to-use retrieval packages were available. Today, auditors also can use other software retrieval language tools that are available on many computer systems.

EXHIBIT 21.1 Programming Steps for Developing a CAATT Application

1. Define overall CAATT objectives: What do we want to test, and why?
2. Identify key applications, database files, key transactions, and cycle times that will test the audit objective.
3. Identify available audit software tools for performing the test.
4. Identify specific files and other data elements that will be tested.
5. Using audit software tools, develop procedures to perform the desired audit tests.
6. Test CAATT against a sample set of production files, and modify the process until it is working properly.
7. Determine timings and key planned updates, and perform the actual audit CAATT test.
8. Follow up on any unusual or unexpected results, and make further corrections as necessary.
9. Report CAATT audit results.
10. Document overall audit results and the CAATT process.

(b) Report Generators Languages

In years past, when IT departments developed their applications, using compiler-based languages such as COBOL, end users relied on the IT department for all of their reports and applications. This dependency on the IT department has very much changed in today's era of desktop computing and powerful user-controlled tools. Today, end users with minimal training regularly produce special reports or perform complex file manipulations in addition to conventionally programmed applications with report-generator languages. Internal audit needs to develop an understanding of the types of generalized retrieval languages available at any auditee location. These retrieval and report generator tools are generally available for most IT environments, from legacy mainframes to laptop computers and even small, handheld wireless devices. Some of these software tools are designed to operate only as a query language for a given database or vendor's application software package. They are often called *report generators* or *query languages.*

Others are quite general and can be used with many applications. The most general and flexible of these are computer languages where only very general instructions are necessary to produce a desired report rather than the detailed steps in a complete computer program. For example, these systems produce an indexlike list of all of the data items available. A program author needs only to select items from those index lists to produce a fairly professional-looking output report. These retrieval languages take care of most other report editing and formatting functions.

Software that comes with a query or report-generator language can satisfy many internal audit reporting needs. For example, a fixed assets control application may have a report-generator subsystem to allow customized fixed assets reports. Auditors should consider using these same report generators for audit retrieval purposes. Many are easy to use. Otherwise, vendors will provide training in the use of the software when it is installed. Even if internal audit plans to use its own generalized audit software, these report-generator products can be very helpful for audit analysis projects.

Since the early 1980s, there have been numerous data retrieval–products, some for end user report-retrieval purposes and others primarily for use by the IT function, such as overall applications generators. Many can be powerful tools for

auditor-developed CAATTs. There is no one single definition of these auditor-friendly retrieval languages, but most exhibit one or more of these characteristics:

- **Nonprocedural language.** Earlier programming languages required the programmer to follow a fixed sequence of instructions to accomplish a given task. For example, a COBOL program producing an output report must first open and read the input file, then select and sort items of interest in order finally to produce the report. This same sequence of steps is not required with a retrieval language. The same example report could be produced with the single instruction "`List data sorted by...`" This makes the software easy to learn.
- **Environmental independence.** Many retrieval languages can be used on a variety of different IT systems environments. They are portable, from laptops to mainframes, operating under different types of computer hardware, operating systems, and telecommunications monitors.
- **Powerful application-development facilities.** Although not necessary for internal auditors, most retrieval languages have powerful facilities to help application developers to design entire systems, including database accesses, "paint" procedures to program retrieval screens, and graphical output reports.

A modern retrieval language offers greater flexibility and ease of use. However, such software products may be expensive and difficult to justify if they are only for internal audit use. Internal audit should investigate and consider using similar tools installed elsewhere within the enterprise. This software typically is licensed to the overall enterprise; internal audit would be one additional user.

Generalized retrieval software can almost always be used for audit retrieval purposes. It has the disadvantage that it does not have such built-in audit software functions as statistical sample selections or serial number gap detection. However, it will work quite well for item selections, recalculations, file matching, and data-reporting purposes. Many specialized audit functions can be coded into the retrieval language with little difficulty.

Many software products come delivered with some type of vendor-supplied retrieval package. For example, accounting software packages for general ledger accounting often come with their own report-retrieval packages. Even specialized commercial software, such as a system to control inventory in a computer center media library, comes with its own specialized retrieval software. This specialized retrieval software often is useful to an internal auditor for accessing and analyzing the particular data records.

A major disadvantage with the various retrieval products included in commercial software is that an internal auditor, in a larger enterprise, may have to learn the report-generation language from multiple software products, none of which may follow a consistent syntax. There may be one or several such products installed on the centralized computers, with additional ones on divisional servers or local workstations. Even though the learning curve for writing audit retrievals with these products is typically short, internal audit may encounter both training and logistical difficulties. Laptop system audit packages, discussed in the next section, can provide internal audit with a single software retrieval product for use throughout the enterprise. However, audit objectives will determine what type of audit software it is best to use.

(c) Desktop and Laptop CAATTs

Desktop computers have had a very significant impact on IT since the introduction of the Apple II and IBM personal computers in the early 1980s. Modern versions of these systems are pervasive in enterprises today either as freestanding devices or, more typically, networked together and to central servers. Laptop or desktop computers are useful tools for developing CAATTs, and several excellent commercial audit retrieval products are available. In addition, other certain standard desktop software products can also be used for audit retrieval purposes to access or download data from larger computer systems and bring them to internal audit's laptop computer.

Internal auditors often wish to examine and analyze the contents of data files located on various remote computer systems within the enterprise. Generalized audit software or other retrieval tools may not be available for processing at these remote locations. For example, due to software license restrictions or computer systems incompatibilities, internal audit's generalized audit software may be usable only on the central server systems. Data files from other locations would have to be transported to that central site over the enterprise's communications network. Even if retrieval languages were available at all locations, it might be necessary for internal audit to spend increased travel time and additional resources processing CAATTs at these remote locations. Desktop-based computer audit software tools can solve many of these problems.

Laptop and desktop computer audit software is a type of generalized audit software with many of the functions and features typically found on older mainframe systems. It is not designed to perform audit retrievals against other systems but against original or extract files from larger computer system applications. This software was originally developed for external auditors who need to access files from many different clients and computer systems. Therefore, many products currently on the market have an external auditor emphasis. Public accounting firms have developed software that they sometimes make available to their clients, and commercial vendors market others. One software product that is quite useful in an internal audit environment is called Audit Command Language (ACL).[2]

Internal audit often must extract and analyze data from very large files on mainframe systems with thousands or millions of records. Although an internal auditor needs to access these larger files, sometimes it is more convenient for internal audit to process these data on an audit department system rather than directly on mainframe systems. This larger volume of data can be processed on a much smaller audit desktop computer equipped with a very-high-capacity USB memory stick. These USB memory devices are discussed in Chapter 20. Auditor laptop systems also need a mechanism to read files from mainframe systems, such as a modem or other communications port. This data retrieval approach can be effective provided the mainframe files are not too large and the laptop system has a sufficient hard disk capacity. (An alternative and often better approach is to equip the audit computer with a memory stick or cartridge drive. These devices are not extremely expensive and can be a good addition to a centralized internal audit department machine.) The audit computer can then read from mainframe tapes to process data for the computer audit test. Although many larger data centers are converting to cartridge formats, tape formats will continue to be used for some time.

The actual audit software programs used for the computer-assisted audit procedures have similar functions and capabilities as the generalized audit software

EXHIBIT 21.2 ACL CAATT Programming Example

ACL is a conversational easy-to-use interactive command audit language that the auditor can load onto the microcomputer to access a fairly universal set of computer file structures. Files can be accessed either through an online connection or from a tape file, extracted from the data center that the auditor would access through a special, 9-track tape drive.

As an example of using ACL, assume an internal auditor wanted to recalculate taxes payable account for a situation where the tax rates would be 20, 30, or 50% depending upon the income level. Income less than $5,000 would result in no taxes, and the other income breaks are $10,000, $30,000, and above. An audit analysis program to recalculate those taxes would first require codes to indicate where annual income was located on the tax file. The taxes payable could then be calculated with the following ACL command statements:

```
TAXES_PAYABLE_COMPUTED
0                                          IF INCOME < 5000
          .2   *   (INCOME – 5,000)        IF (INCOME < 10,000)
1,000  +  .3   *   (INCOME – 10,000)       IF (INCOME < 30,000)
7,000  +  .5   *   (INCOME – 30,000)
```

These four commands would read through the file and produce an audit total.

procedures discussed previously. The only limitation sometimes is the memory and storage capacity of such smaller systems. If a large number of data files are to be compared as part of the CAATT, a laptop system may not be that efficient because typically only one tape drive is available.

Exhibit 21.2 describes the programming instructions necessary to develop a CAATT application using the ACL product. In this example, an internal auditor would have secured a copy or extract of the enterprise's accounts receivable master. Using the ACL, internal audit can easily perform this common financial audit task. The idea here is not to show how to write such a program but to illustrate that it is a relatively simple and easy-to-learn task.

(d) Test Data or Test Deck Approaches

The term *test deck* is an old computer audit–related term dating back to the earliest days of information systems, when applications operated in a batch mode and used punched cards as input media. In order to test a computer application, internal auditors developed a series of test transactions that achieved known results. In those early days, these transactions were prepared on a set of input punched cards or a test deck. The term *test deck,* of course, is dated, given today's technology, but it describes a very useful CAATT approach where an internal auditor submits a series of test transactions against a live production system to determine if controls are adequate. (A better expression for this approach is *test data,* although we will continue to use the traditional name.)

For example, internal audit might use a test deck CAATT approach to test controls in a payroll system. Using a copy of the payroll master, internal audit might submit transactions for some known employees showing standard hours of work, for others showing some overtime hours, and for a third group showing an excessive number of hours that internal audit would expect to trigger an error report. A special, controlled run of the payroll system would then be arranged using

these test transactions. Internal audit would subsequently verify that the pay was computed correctly, the files were updated correctly, and all expected error and transaction reports were correct. The audit test transactions would then be purged from the updated files. Through this test deck, internal audit could gain a level of assurance that the payroll system, in this example, was working correctly.

Test deck approaches fell into disuse as systems became more complex and ceased to be batch oriented. However, this approach—which calls for the submission of audit test transactions to a copy of a live application—is still a viable CAATT approach for testing IT applications. An actual deck of test transaction cards is not necessary. Test decks—or, more properly, test data approaches—can be very useful for gathering audit evidence. For the modern computer application, the approach uses a predetermined set of online transactions as the test deck. The CAATT approach allows internal audit to input a series of test transactions through an application input screen to achieve these objectives:

- A general understanding of the program logic associated with a complex system
- A determination that valid transactions are being processed correctly by the application
- A determination that invalid or incorrect transactions are being identified correctly and flagged by the application's program controls

There are limitations in this testing approach. If a given transaction type has not been prepared for the test, internal audit cannot affirm that the application works correctly in respect to that transaction. If the documentation is incomplete or incorrect, internal audit may miss a key transaction test.

Test data CAATTs can also be developed by tracing user-initiated transactions through a normal production cycle or by inputting a series of audit test transactions through a special test run of the application. There are advantages and disadvantages to each of these approaches.

(i) **TRACING USER-INITIATED TRANSACTIONS** An internal auditor sometimes must review and gather evidence of transaction controls for complex IT applications. For example, internal audit may want to verify that some component of an enterprise resource planning (ERP) system is operating with appropriate controls. Such an ERP system generally has numerous programs to control the receipt of materials into a production facility, to add them to inventory, and then later to retrieve them for manufacturing work orders as components of the complete manufacturing process.

These steps require numerous and various transaction types covering multiple processes; they are difficult to assess through audit sample processing. When faced with a complex application, an internal auditor often will be unable to easily identify single points in the application process flows to develop effective CAATTs. A formal test data approach, where internal audit sets up a separate system process, is also difficult due to the overall complexity of the system.

The most reasonable approach to testing may be to trace a representative sample of normal transactions initiated through the production application. Following the example of a manufacturing ERP system, an internal auditor should first identify key control points in the overall system. The next step is to observe and record transactions being entered at each of these points such that they can be traced to the appropriate online screens or reports. As part of this observation, internal audit

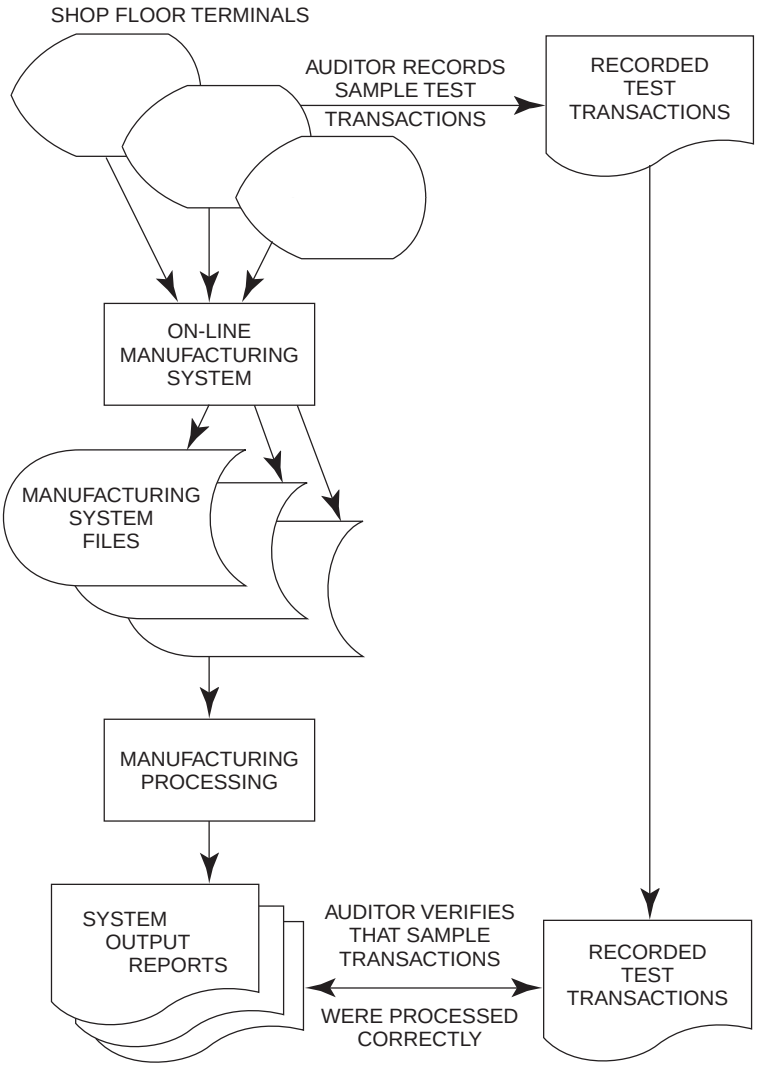


EXHIBIT 21.3 Test Data CAATT Approach: User-Initiated Transaction

may also want to ask users to input certain invalid transactions to ascertain that they have been rejected correctly. Exhibit 21.3 shows this user test data CAATT approach.

The tracing of user-initiated transactions is similar to the transaction walk-through approach for computer applications described in Chapter 19. The difference here, however, is that with this test deck approach, an internal auditor captures a more substantial number of normal transactions for tracing and verification. While this approach is not a true CAATT, it can be combined with other CAATTs at key points to gain a better understanding of the application's processing procedures and of its controls. For example, internal audit can trace input inventory transactions through a manufacturing system. Combined with a CAATT, these selected transactions could then be used to compare beginning and ending period inventory status files to highlight the differences caused by the production online transactions.

A test transaction procedure is more of a manual testing technique than a true CAATT. It also emphasizes transaction input processing and the resultant outputs around the computer system rather than the actual operations of the component programs. Often it is not the best way to gain positive assurance that an application is working with all of the proper controls. However, it can be an effective way to gain a level of assurance that the application appears to be working with no obvious errors. While individual programs can be tested in some detail, tracing user-initiated transactions may be the only way to test an entire operational application.

(ii) APPLICATION TESTS USING TEST DATA This CAATT approach uses auditor-prepared test data transactions or test files. If an application has only one key input point, auditor-initiated test data entered through that point for processing in a special run often is an effective CAATT. For example, an enterprise may have an online labor time collection system where employees input hours on a single-screen format for recording time and allocating the hours to various projects. Internal audit may be interested in verifying the integrity and correctness of the output data here.

An approach to testing this type of system is to build an audit file of representative test transactions for input to a special test run. These transactions should represent different valid and error conditions to allow internal audit to test as many conditions as possible. Live files or copies can be used for all processing. The auditor's file of test transactions is input to this test run, and internal audit subsequently verifies the results of the systems processing. The test data approach can be an effective type of CAATT to gather evidence about smaller, self-contained IT applications. Rather than using audit software to develop retrieval reports showing file contents, this technique allows internal audit to test program logic by passing or submitting test transactions against a set of live data files and production programs to verify the correctness of application processing. In the user-initiated transaction approach discussed previously, an internal auditor reviews the results of an actual production transaction. This test data approach allows the auditor to develop a series of can't-happen transactions to determine how systems controls are working in these extraordinary situations. This approach, however, has some limitations:

- The IT operations function sometimes objects to internal audit's request to process a special run of a production application for fear that the audit test data will somehow become intermingled with and corrupt the normal production data.
- Test data can test only one cycle of an application effectively. Due to the IT operations disruptions this CAATT generally causes, it is usually difficult to schedule multiple test cycles.
- The approach is cost effective only for more self-contained applications since it is difficult to design test data covering multiple input points.
- Preparing a comprehensive set of test data often is more time consuming than preparing a conventional CAATT retrieval program.

Despite these limitations, a test data approach is useful when internal audit reviews an application that has been implemented at multiple locations within the enterprise. By developing a standard set of test data and using it at each of the locations, internal audit can verify, among other things, that there have been no unauthorized changes to the application programs at remote locations.

(e) Specialized Audit Test and Analysis Software

Internal audit often has a need to review specialized IT system files, such as those associated with the computer operating system or online transaction log files. This requires a very different type of CAATT from what internal audit would develop for financial and operational application audit tests. Because computer operating systems and related files generally are very complex, generalized audit software often will not work. Generalized audit software works best with conventional files defined in fixed record and field lengths; systems software files use very specialized file format structures.

An internal auditor is sometimes interested in monitoring the integrity of the mainframe computer's operating system or related parameter files. For example, IBM's System 390 z/OS operating system, used on legacy system mainframe computers, contains numerous library files and parameter tables, which could be manipulated to allow security and integrity violations. Specialized audit analysis software can be used both to access these files and to identify potential operating system integrity exposures.

Creative and technically skilled auditors can use other specialized software tools to develop unique CAATTs. Many are not specifically designed for auditors but for normal computer systems developers or end users. However, internal audit can often make very effective use of them. Some of these tools are listed next.

- Manufacturing production and materials scheduling software packages often contain ad hoc reporting subsystems to analyze their application files. Internal audit can use them to extract a sample of production part numbers for further testing.
- Software to control the movement of IT storage media in and out of the library often has an ad hoc reporting capability. With minimal training, an internal auditor can use these report-generator packages to test library operational and media management controls.
- Applications programmers frequently use computer-aided systems engineering (CASE) software tools to help them build more effective new applications. CASE software also can be a very effective audit tool for developing process flowcharts and documenting applications.

Although typically not considered CAATTs, numerous ad hoc retrieval and analysis software packages can aid internal audit. Because such software often is easy to learn and use, internal audit need just needs to ask if it is available when reviewing a specialized area or application. In other instances, internal audit may need to acquire certain specialized software tools to support audit efforts.

(f) Embedded Audit Procedures

Most conventional CAATTs require an internal auditor to initiate some action to start the testing process. The CAATT will identify the condition only when it is processed as part of a scheduled, periodic audit. However, internal auditors often are interested in monitoring exception transactions within an application on an ongoing basis. Embedding audit software into a production application can provide continual monitoring for activities of interest and report them for immediate or subsequent audit analysis.

This embedded audit procedure approach is called an integrated test facility (ITF), an internal audit–established, built-in test data facility. In many respects, a continuous, embedded audit monitor is similar to the error- or exception-reporting mechanisms built into many conventional applications. It is also similar to the log file approach used for monitoring activities through a computer operating system. The major difference is that conventional application exception reports usually log all such problems and system log files record all activities. A continuous audit monitor logs and reports only items of predetermined audit interest. Also, application exception reports and system logs typically have a wide distribution; audit monitors are reports for the exclusive use of internal audit. This general continuous audit assurance approach is discussed in Chapter 29.

Both continuous audit monitors and ITFs allow internal auditors to have access to certain automated system conditions on an ongoing, continuous basis. Internal audit needs management support and commitment to devote audit resources to this type of effort. If implemented, these types of embedded audit procedures will have an expanded role in the enterprise's overall system of internal accounting controls.

(i) CONTINUOUS AUDIT MONITOR DESIGN AND IMPLEMENTATION As an example of a continuous audit monitor, assume that an auditor is working in a multibranch financial enterprise with numerous transactions between the branches. Internal audit has reviewed the significant financial applications to test internal controls and has used generalized audit software to test key elements of the financial applications. However, the internal auditor is interested in monitoring and following up on certain exception transactions that may be initiated by various branch users from time to time.

The example application has a large number of exception reports for user follow-up; internal audit is interested only in reviewing certain large-value interbranch transactions above a specified dollar limit. While normal operational personnel should also follow up on such transactions, an internal auditor might be interested just in the nature of such transactions and the level of follow-up activity. A continuous audit monitor CAATT can allow internal audit to review these ongoing exception transactions.

A continuous audit monitor CAATT is a special, auditor-defined program that gathers evidence about transaction exceptions or potentially unauthorized items that may require auditor follow-up. This type of a monitor will not allow internal audit to perform detailed tests of an application but will collect the transaction data for subsequent testing and analysis. Because it must be built into a production application, a continuous audit monitor CAATT should be installed only where internal audit has a strong, ongoing review interest.

Continuing with this example, after internal audit gains a detailed understanding of the application and identifies where the interbranch transactions of interest can be captured, it should request that the IT function insert program code into the application to monitor and capture all such transactions of interest. These monitors are normally written onto a protected log file for later audit review and analysis. Exhibit 21.4 illustrates how such a continuous audit monitor might be constructed.

Because a continuous audit monitor is an embedded set of program code, it cannot be changed easily. Internal audit should design the objectives and selection criteria associated with any such monitor carefully. Properly constructed, however, it can be an effective tool to independently monitor applications where internal audit has an ongoing interest. There are some potential problems with this approach. In

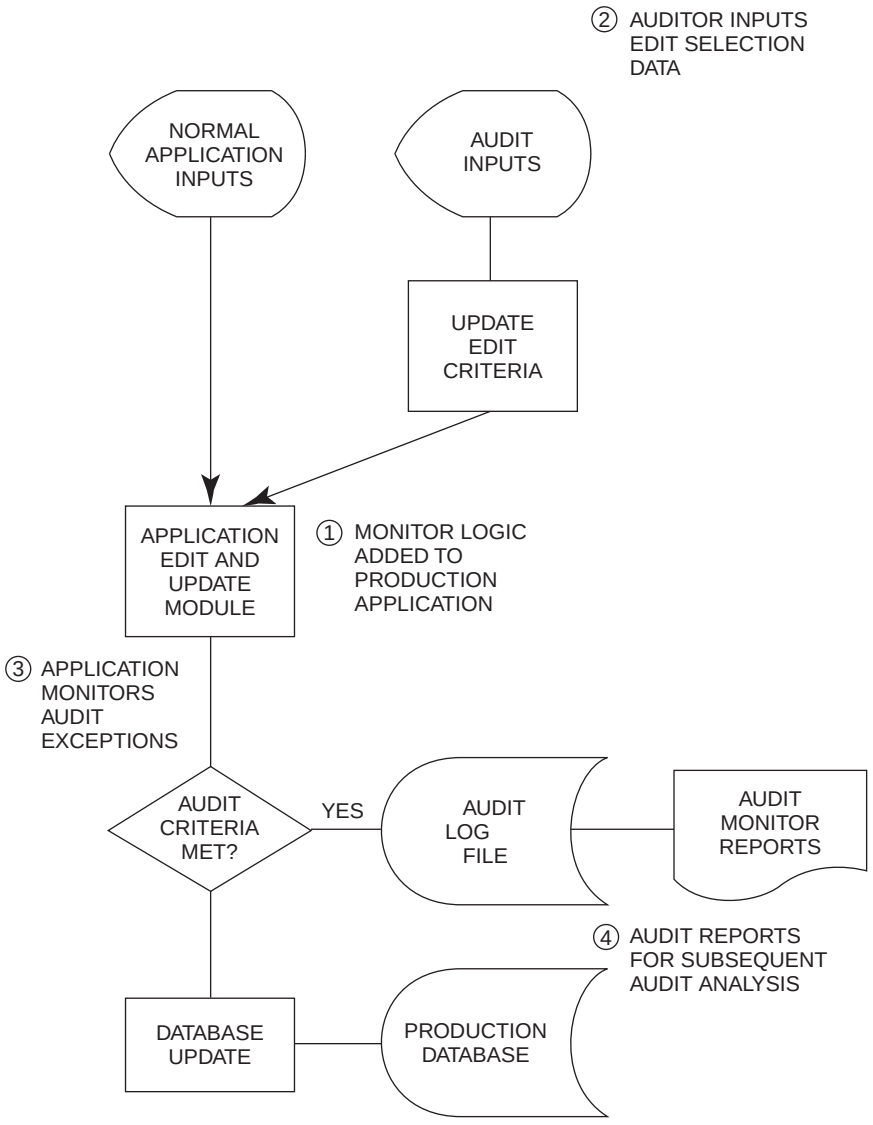


EXHIBIT 21.4 Continuous Audit Monitor CAATT Approach

particular, internal audit is generally not able to implement such a procedure independently and needs IT assistance to build a monitor into a production application.

The other CAATTs discussed in this chapter often can be established fairly independently by internal audit. Given an understanding of data file structures, internal audit can use generalized audit software to perform various tests. Likewise, many test data procedures can be established independently. This is not true for the continuous audit monitor, which must be embedded into a normal production application. Internal audit normally will need to work with the IT application development function to define the requirements of a monitor. The most efficient time to suggest the implementation of such a monitor is when an application is being developed.

If appropriate, internal audit can request that a continuous audit monitor be installed as part of a review of the system under development. Installing a continuous audit monitor in an application already operational is more difficult because it may require changes to other associated application procedures. Internal audit should also recognize that because the IT function installs such a monitor, it will be aware of it and may have the ability to bypass its monitoring functions. Nevertheless, a continuous audit monitor can be a powerful tool to review certain exception items associated with critical transactions. Although the example cited was for a financial application, the procedure is applicable to many other types of nonfinancial applications. In a manufacturing enterprise, internal audit could install such a monitor to log and report, for example, all scrap disposals above a specified limit.

(ii) INTEGRATED TEST FACILITIES An ITF is an embedded program module that allows an auditor to test an application on an ongoing or random basis. It differs from the continuous audit monitor, which records all production transactions of a certain activity or type. An ITF records only special test transactions that internal audit has independently input to the application. An example might better explain how an ITF is constructed and used. Similar to the continuous audit monitor example, assume that internal audit is interested in reviewing controls over a central financial system covering a large, multidivision enterprise. That central financial system receives transactions from its operating entities for both internal and interdivision financial entries. Each division included in the financial application is identified by a unique division code. In addition, the central organization accounting function initiates transactions that affect all operating entities. An internal auditor may be interested in the controls over these various transactions as well as in any potentially improper accounting items.

An ITF allows internal audit to review this application on an ongoing basis. Internal audit might set up a dummy division number—such as Division Code 99—in the application's authorization files. All system reports for this Division Code 99 are then routed to internal audit to test transactions against this code for system accuracy and program integrity. In addition, if other normal transactions impact all divisions, internal audit would be able to review them on the Division Code 99 reports. Exhibit 21.5 illustrates how such an ITF might be constructed. An ITF can be an effective test data type of CAATT for many forms of applications.

A special test run is not normally required with an ITF as auditor transactions are entered with other normal transactions. As with other CAATTs, however, ITF transactions can then be compared to predetermined processing results in order to gather evidence about the application being tested. Internal audit can construct an ITF using two alternative approaches. First, the basic IT application can remain unchanged, with internal auditors only inputting transactions against the designated auditor code—such as the Division Code 99. These transactions must be purged from the system only after the testing has been completed. For an accounting application, purging sometimes can be as simple as entering reversal transactions to the system. However, often the reversal process is much more complex. For example, many accounting systems have allocation processes that may affect all balances in the system; it is important that internal audit's ITF test data does not cause other account balances to be altered. A second approach to building the ITF is to add a program process to filter out any audit transactions. This way, internal audit's test transactions can be transparent to other system users. The problem with this method is the

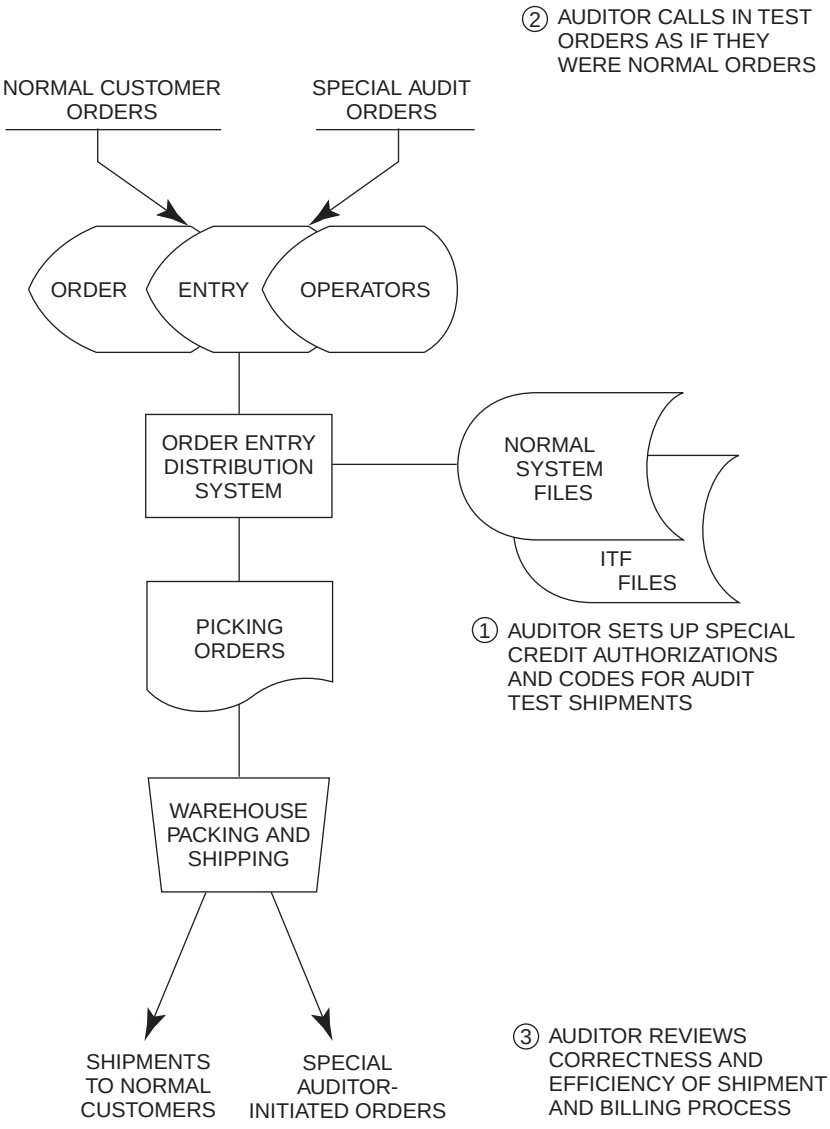


EXHIBIT 21.5 Integrated Test Facility CAATT Approach

special programming required to build the filter. If the IT department is one of the functions being examined, the integrity of the tests could be compromised.

In either event, an ITF is an advanced approach to testing and gathering evidence about an automated application. Because of the program coding and logistics required to establish an ITF, the technique is difficult to establish and should be used only when internal audit has strong, technical skills and an ongoing interest in reviewing an application. In addition, an internal auditor responsible for implementing the ITF should have a thorough understanding of all aspects of the target application before beginning ITF. Otherwise, the ITF transaction activities may have unintended effects.

Several other areas of caution should be considered before constructing an ITF. In some regulated industries—such as financial institutions—auditors may be in violation of state or federal statutes by establishing fictitious accounts in financial applications. Internal audit should discuss any ITF plans with the enterprise's counsel, if appropriate. Internal audit should also make certain that only a limited number of personnel are aware of the ITF. If it is generally known, for example, that Division Code 99 is internal audit's number, anyone making improper transactions will take steps to see that the code is bypassed.

21.4 Selecting Appropriate CAATT Processes

Although CAATT tools, such as ITFs, offer some opportunities for special audit monitoring, internal audit is usually better off using generalized audit software, such as ACL, or similar retrieval software for many of its CAATTs. The approach to use depends very much on the IT environment, the availability of software tools, auditor technical knowledge, and, most important, internal audit's CAATT objectives. In a larger IT environment with a centralized IT function, generalized audit software is often the preferred alternative. It offers some of these advantages:

- **Fast learning curves.** Auditors with even limited IT knowledge can easily build audit test and retrieval applications.
- **Preprogrammed audit functions.** The software generally has functions of audit interest, such as gap sequence number checking, built in.
- **Limited coding requirements.** Although the software is primarily designed for simple, quick-and-dirty retrieval reports, effective CAATTs can be produced with very few programming steps.

In addition, a report generator is often the most cost-effective CAATT tool for many internal audit functions today. Often internal audit can use and share the costs of a report generator software package used in various parts of the enterprise. Many report generator retrieval tools can accomplish most of internal audit's CAATT objectives despite their lack of specialized audit functions.

Desktop system audit software provides some unique advantages in many situations. Files can be downloaded to an auditor's computer within the audit department rather than having an internal auditor work directly in IT operations. The decision of which CAATT software to use depends very much on overall audit objectives. Internal audit should consider the appropriate type of audit software, depending on overall audit objectives, the equipment environment, auditor IT skill levels, and budget constraints.

21.5 Steps to Building Effective CAATTs

Internal auditors should follow the same general approaches for developing CAATTs, whether they use generalized audit software, a report generator retrieval language, or download data to a laptop computer. This approach is similar to the application development processes discussed in Chapter 19. The difference here is that an internal auditor may develop a CAATT for a one-time or limited-use effort rather than

for an ongoing production application. Because internal audit often draws conclusions and makes significant recommendations based on the results of a CAATT, it is important to use good systems practices to design and test CAATTs. A four-step approach to develop a CAATT is described next.

Step 1. Determine the CAATT's audit objectives. It is not sufficient for internal audit just to audit an automated accounting system. All too often an internal audit manager just directs a staff auditor to write a CAATT for some audit without fully defining its objectives. The desired audit objectives should be defined clearly; this will make the subsequent identification of testing procedures much easier. Once internal audit has defined its CAATT objectives, file layouts and systems flowcharts should be obtained to select the appropriate data sources for testing. Sometimes at this point an internal auditor encounters technical problems that might impede further progress. A CAATT documentation file or workpaper should also be started along with this step.

Step 2. Design the computer-assisted application. The CAATT software tool used must be well understood, including its features, overall program logic, and reporting formats. Any special codes or other data characteristics must be discussed with persons responsible for the computer application. Consideration should also be given to how internal audit will prove the results of audit tests by, for example, balancing to production application control totals. These matters should be outlined in the documentation workpapers.

Step 3. Program or code and then test the application. This task usually follows Step 2 very closely. Programming is performed using the generalized audit software or some other selected software tool. Once the CAATT has been programmed, internal audit should arrange to test it on a limited population of data. The results must be verified for both correctness of program logic and the achievement of desired audit objectives. This activity should also be documented in the workpapers. Correctness of program logic means the CAATT must *work,* but sometimes an error in coding will cause the application to fail to process. The failure to achieve audit objectives is a different kind of problem. For example, in a CAATT to survey conditions in an inventory file, an auditor may make too broad of a selection, producing an output report of thousands of minor exceptions. Such CAATT logic should be revised to produce a selection of a more reasonable size.

Step 4. Process and complete the CAATT. Making arrangements for processing the CAATT often requires coordination between internal audit and IT operations. Internal audit often is interested in a specific generation of a data file, and it is necessary to arrange access to it. During the actual processing, internal audit must take steps to ensure that the files tested are the correct versions.

Depending on the nature of the CAATT, an internal auditor should prove the results and follow up on any exceptions as required. If there are problems with the CAATT logic, internal audit should make corrections as required and repeat the steps. The CAATT application workpapers should be completed at this point, including follow-up points for improving the CAATT for future periods.

Computer-assisted audit techniques are powerful tools that can be used by any internal auditor and should not be solely the responsibility of an IT audit specialist. Just as end users make increasing use of retrieval tools for their own IT needs, all members of an audit department should gain a CBOK understanding of available audit tools to allow them to develop their own CAATTs.

Of course, as more and more automated processes become paperless, the auditor's need to build and use CAATTs will increase. Today's modern automated system reduce or even eliminate the traditional paper trails that auditors use to trace and validate transactions. Audit tools ranging from generalized audit software to continuous audit monitors will increasingly become the only options available to test and gather evidence about these paperless systems. Many operational systems have some very strong paperless elements. For example, either Web-based systems or the automatic teller machines used by financial institutions have very limited paper trails; the only way to audit such applications effectively is through the use of CAATTs. An internal auditor must be creative when designing a CAATT to gather evidence regarding these paperless applications, and many of the techniques described in this chapter apply.

21.6 Using CAATTs for Audit Evidence Gathering

When reviewing automated applications, internal auditors often do not give sufficient attention to the need to gather evidence. Many times it is an interesting and challenging audit task to gain an understanding of an automated application and to evaluate its internal controls. However, some internal auditors consider detailed confirmations of account balances or other types of evidence-gathering tests as not as interesting and too time consuming. These evidence-gathering procedures often provide internal audit with opportunities to implement the most creative portion of the audit project. Assume, for example, that internal audit has performed detailed internal controls–oriented review of a large fixed-asset capital budgeting application where transactions are initiated from a variety of subsidiary systems and where the application eventually provides general ledger financial statement balances. Internal audit has tested system-to-system internal controls and concludes that they are adequate; it also has manually recalculated the depreciation expenses for several selected transactions and found them to be correct.

Can an internal auditor conclude that the fixed assets and accumulated depreciation numbers produced by this sample system are accurate? In a large enterprise, where fixed assets may represent a substantial portion of the balance sheet, an internal auditor may decide that relying solely on this internal controls review presents far too great of a risk. The several transactions selected for a recalculation compliance test may not be representative of the entire population, and there may be an error in certain classes of these transactions. Although application-to-application controls may have appeared proper, some types of transactions may be assigned to incorrect account groups. Without detailed CAATT-based testing of this example system, it is possible that these errors could go undetected.

Internal auditors should have an understanding of when it is cost effective and appropriate to develop CAATTs to perform detailed tests of IT applications in order to verify the correctness of transactions or account balances. Some circumstances

when internal audit should perform this more detailed application evidence gathering and testing include:

- There is a perception that the risk of relying just on internal controls is too high.
- Although internal audit may have performed limited walk-through or compliance types of tests, the results of those tests may be somewhat inconclusive and suggest a need for more detailed tests.
- In some instances, certain internal controls may be weak or difficult to identify; and internal audit may want to develop CAATTs to perform detailed tests of the automated applications.
- Some complex or large automated applications are involved, such as comprehensive ERP systems.

In many instances, audit management decides whether to rely just on internal accounting controls and limited compliance testing or to perform detailed tests of transactions. However, the use of CAATTs should be a key internal audit tool in many situations. The nature of the audit tests to be performed, the extent of data, the complexity of the application, and the tools and skills available to internal audit should all be factors in this decision. Internal audit should become familiar with the various software products and techniques available for analyzing and testing computer system files. A general understanding of the implementation and processing of CAATTs should be part of the CBOK skill set requirements for all internal auditors.

Notes

1. American Institute of Certified Public Accountants, *Computer-Assisted Audit Techniques* (New York, 1979). This auditing guide is now out of print.
2. ACL Services Ltd., Vancouver, B.C., Canada; www.acl.com.

CHAPTER 22

Business Continuity Planning and IT Disaster Recovery

Virtually all enterprises today would not be able to function without their information technology (IT) systems and the supporting communication networks, data repositories, and overall IT infrastructure. However, those same IT systems could be subject to any of a wide range of failures. The enterprise needs to have facilities and resources in place to recover and restore IT operations in a prompt and orderly manner. In IT's earlier days, this was called disaster recovery planning, and the emphasis was on the recovery of computer systems, applications, and data files.

Enterprises have regularly established disaster recovery procedures for keeping backup versions of older computer files and programs in secure locations along with processes for restoring those backup files if a disaster event limited access to current versions. While earlier backup processes were often based on fairly simple systems configurations, today's network-based integrated systems have made backup and recovery much more complex. In the years up to the beginning of this century, internal audit often reviewed established backup procedures and found them weak. Processes for strong business continuity planning often were very limited and lacked adequate testing. However, despite frequent comments in internal audit reports over the years, the issue often did not receive much high-level management and audit committee attention.

September 11, 2001, changed everything. Two airplanes crashed into the two 100+-story New York World Trade Center towers, causing the buildings to collapse. Another plane crashed into the Pentagon in Virginia. In addition to a massive loss of life and property, these events triggered activation of a series of enterprise IT disaster recovery plans. The World Trade Center was populated with a large number of IT systems-based financial institutions, most of which had what were thought to be adequate IT disaster recovery plans in place, but many of those were later found to be wanting. In the immediate aftermath of the 9/11 disaster, telephone lines were clogged, bridges to Manhattan were closed, and airlines were shut down. Many of the IT disaster recovery plans in place just did not work. Only a few enterprises had disaster recovery plans that were effective.

This chapter introduces best practices for effective IT business continuity and disaster recovery planning for internal auditors to use when reviewing internal controls in this enterprise-critical area. In past years, internal audit often was one of the few voices raising disaster recovery concerns. This internal audit role continues today. In addition, many U.S. federal regulations now contain requirements for

effective IT business continuity and recovery programs, and management at all levels generally recognizes the need for such provisions. Along with other groups such as legal and IT security, internal auditors continue to have a key role in reviewing, testing, and evaluating their enterprise's business continuity planning.

The chapter also briefly introduces some of the technical tools that improve business continuity procedures today. Although the discussion of these recovery tools is not in depth, areas where an internal auditor should, at least, have a general understanding are described. For example, the chapter introduces data mirroring techniques (a process where duplicates of IT application transactions are immediately routed to another site). Internal auditors certainly do not need to understand the technical configurations of data mirroring but should have enough knowledge to ask some high-level questions about whether it has been considered.

This chapter concludes with a discussion of BS 25999, a British-based standard for business continuity management. Although not yet a full worldwide standard, these U.K. standard may soon evolve into an international standard for continuity management. (In Chapter 30, we discuss the evolution of ISO worldwide standards.) An internal auditor is not expected to have a detailed, specific common body of knowledge (CBOK) level of knowledge regarding these BS 25999 standards or the new technologies for effective business continuity planning. However, a basic understanding of IT business continuity planning processes is an important internal audit CBOK skill.

22.1 IT Disaster and Business Continuity Planning Today

Over the years, internal audit reports have discussed the risks of an enterprise losing a substantial element of its IT resources due to some disaster event. Many of these internal audit concerns go back to the early days of IT with centralized data centers, but raising the issue of internal audit risks to both IT and senior management then was often a hard sell. This author recalls leading an internal audit of disaster recovery planning for a then major U.S. corporation in the early 1990s, where one of its major data centers was located close to a high-traffic airport—with the risk of an airline incident—and where there was no effective IT recovery plan in place. When internal audit concerns about the lack of an effective IT recovery plan were first raised, the corporation's chief information officer (CIO) shrugged it off, saying such as disaster could "never happen." In the end, internal audit had to raise these concerns in a meeting with the audit committee to get the corporation to launch such an IT disaster planning effort.

Throughout the 1980s and early 1990s, a common IT disaster recovery solution was to make arrangements with a remote disaster recovery data processing facility to handle any emergency processing. Key backup files and programs were stored at offsite locations, with plans calling for the IT staff to shift to that alternate facility in the event of a disaster event. Professionals thought of IT disasters just in terms of fires, floods, or other bad weather situations. In those earlier, primarily mainframe systems days, enterprises sometimes even took what today sound like rather bizarre actions for developing their IT disaster recovery plans: They signed "reciprocal agreements" with nearby locations having similar IT resources so that each could move to that other location for processing in the event of an emergency at either. Reciprocal agreements between two CIOs then sounded good in theory, but they have never

really worked beyond low-level, almost humanitarian help. That nearby reciprocal agreement site might be out of service for the same weather-related disaster or probably would not be interested in another company running its systems in off-shift time periods. As a final impediment, an enterprise's legal counsel would have a dozen reasons to say no to a reciprocal agreement.

Others established raised-floor vacant space at one of their facilities and secured an agreement with their computer system hardware and network providers to move in a replacement system in the event of an emergency. Computer hardware vendors will still agree to replace equipment in the event of an emergency. In fact, this process is easier today as computer hardware is usually off-the-shelf rather than being mostly custom manufactured, as was common in the past.

Those disaster recovery plans often were not sound. A series of specialized disaster recovery vendors soon appeared with fully equipped computer systems sites operating at idle or what is called a "hot" site to serve as an emergency backup facility. They are called hot sites because the mainframe IT equipment ran at idle and was ready to service an emergency client. In those days of centralized IT facilities, enterprises contracted to use those sites as their disaster recovery facility, ran periodic tests, and kept key backup files there. Even though technology changes have caused some challenges to these disaster recovery operations, these specialized hot-site backup vendors still provide the primary IT backup solution for many enterprises moving into this twenty-first century.

In today's era of client-server and Web-based applications, an enterprise faces a new set of risks around its IT assets. Typically there is not one major or central computer facility for handling major automated applications but a wide range of desktop devices, servers, and other computer systems connected through often very complex communications, storage management networks, and links to the Internet. Enterprises do not have all of their IT resources tied around one or several central data centers, and management is more interested in keeping its IT up and running rather than worrying about the risk of losing a central computer systems facility. The concept of IT disaster recovery planning, going back to the 1970s, was based on having processes in place to resume operations if some single disaster made the computer center inoperable. The frequent complex and lengthy mainframe computer start-up process is not true today, but an enterprise needs to establish robust business continuity processes when faced with unexpected events.

The language and strategic approaches to IT business continuity and disaster recovery planning has changed today. While we certainly cannot deny that the events of 9/11 represented a major disaster, professionals today more typically think in terms of the importance of a business continuity plan (BCP), the procedures and processes necessary to restore overall business operations. The user of an online order processing system cares less about whether the server is operating but if a customer order, submitted through an Internet site, can be processed properly and efficiently. The application should be restored and operating as quickly and efficiently as possible, but the key objective is to support and restore the business processes.

In addition to concerns about restoring operations in the case of some disaster or business continuity event, enterprises today are also concerned about the continued and high availability of their IT resources, recognizing that any form of IT systems downtime can be very costly to an enterprise. The Web is filled with estimates of the business cost of IT downtime to an enterprise. For example, several years ago the Disaster Recovery Institute[1] estimated that the average hourly impact of an hour

of systems downtime, for example, is $89,500 for an airline reservations system or $2.6 million for a credit card authorization provider. Beyond just estimates, eBay's Internet auction site went down for 22 hours in August 1999. This caused $4 million in lost fees and a $5 billion drop in eBay's market value.[2] A systems failure will interrupt normal business processing, but a disaster that causes the loss of key records can be even more severe. The message here is that high systems availability and business continuity are very important to an enterprise, and internal auditors should continually look for areas where they can suggest continuity planning and IT availability improvements. The next sections outline suggested internal audit activities and procedures for BCP, a step forward from the older, more traditional IT disaster recovery planning.

22.2 Auditing Business Continuity Planning Processes

Internal auditors should always look for the existence of a current and tested BCP, whether they are performing a review of general controls over an office server system, of a major IT operation, or of a desktop spreadsheet application used for office records, With the strong IT management awareness to have some levels of processes in place, internal auditors generally will not be breaking new ground when they look for the existence of BCP procedures. Too often these procedures find them out of date, not tested, or just ineffective.

Here we describe procedures for internal audit BCP reviews from the perspectives of a centralized IT operation serving multiple units in an enterprise; a single but smaller server lever system serving a business unit; and BCP procedures for a smaller, individual system, such as a financial analysis system on a key manager's laptop system. The objective of each of these environments is to ensure that business continuity processes are in place. Although there is always room for improving these processes, the internal auditor's role in each of these descriptions should be to assess the adequacy of BCP procedures and to make effective recommendations.

No matter the size of the IT environment and its business operations, an internal auditor must develop a good understanding of the relative risks associated with a loss or unexpected interruption in services, the technologies used and employed, and the technical and business nature of the environment. While there is really no one-size-fits-all here, an internal auditor needs to understand the BCP environment and the nature of ongoing testing and evaluations in order to make appropriate internal audit recommendations.

(a) Internal Auditor Centralized Data Center BCP Reviews

A BCP is an outline of the steps necessary to help an enterprise recover from major service disruptions, whether a fire or serious weather emergency, a computer equipment or network equipment failure, or any other form of major disruption. The goal of a BCP is to help an enterprise reduce the impact of a disaster-related outage or extended service interruption to an acceptable level and to bring business operations back. As discussed, a BCP represents a change in emphasis from what IT professionals formally called a disaster recovery plan. The prime emphasis of those older plans was to recover computer systems and data processing operations; the BCP emphasizes needs for continuous operation of the business unit.

As discussed, while IT operations functions have had published disaster recovery plans in place for some time, those older approaches often not that effective in getting key business processes operating again. Just as there are key separate steps necessary for planning and for conducting an internal audit, there are some key steps necessary for an effective BCP. Several professional enterprises, such as the U.S. based Disaster Recovery Institute and its London-based counterpart, have adopted a set of 10 BCP recommended professional practices as outlined in Exhibit 22.1. These are the universally accepted standards in the industry for the key steps in a BCP, and the next sections discuss some of these steps in greater detail. An effective BCP

EXHIBIT 22.1 Key Steps to Building a BCP

1. **Project initiation and management.** BCP processes should be managed through formal project management processes and within agreed time and budget limits.
2. **Risk evaluation and control.** A formal BCP risk evaluation process should be used to determine events that can adversely affect the organization and its facilities with disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss. This process should include a cost-benefit analysis to justify investments in controls to mitigate these risks.
3. **Business impact analysis.** Managers should understand the overall impacts resulting from disruptions and disaster events that can affect the organization as well as techniques that can be used to quantify and qualify them. Doing this requires establishing critical functions, their recovery priorities, and interdependencies such that recovery time objective can be set.
4. **Developing business continuity strategies.** One single BCP is not applicable for all circumstances, and management should develop a strategy to determine and guide the selection of alternative strategies for recovery of business and information resources within the recovery time objective while maintaining the organization's critical functions.
5. **Emergency response and operations.** Emergency procedures should be in place to respond to and stabilize the situation following an incident or event, including establishing and managing an emergency operations center to be used as a command center during the emergency.
6. **Developing and implementing business continuity plans.** The BCP should be developed, documented, and implemented using a formal, best practices–based process that provides recovery within established recovery time objectives.
7. **Awareness and training programs.** Processes should be in place to make all members of the organization aware of the BCP procedures in place with training programs established.
8. **Maintaining and exercising business continuity plans.** The BCP and its key elements should be kept up to date with periodic testing of critical plan elements. Processes should be implemented to maintain and update the BCP in accordance with the organization's strategic direction.
9. **Public relations and crisis coordination.** Processes should be in place to communicate all events surrounding a contingency event and to communicate with and, as appropriate, provide trauma counseling for employees and their families, key customers, critical suppliers, owners/stockholders, and corporate management during a crisis. All stakeholders should kept informed on an as-needed basis.
10. **Coordination with public authorities.** Processes should be in place for coordinating continuity and restoration activities with local authorities while ensuring compliance with applicable statutes or regulations.

Source: These recommended professional steps were developed initially by the Disaster Recovery Institute.

is critical for an enterprise, and management is responsible for the survivability and sustainability of total operations to serve customers and service recipients. Many companies and most government enterprises are required by law to develop IT business continuity plans. In some instances, legislation effectively requires a BCP. The Sarbanes-Oxley Act (SOx), for example, requires registered enterprises to report their financial results in a timely manner. A systems failure is not an excuse, and an effective BCP will help to support the enterprise here.

(i) BCP PROJECT MANAGEMENT, RISK ANALYSIS, AND BUSINESS IMPACT ANALYSIS We have combined the first three elements of Exhibit 22.1 to one internal audit step. When reviewing the BCP in place for an IT unit, internal auditors normally will not be involved in the very important project management processes to build such a plan. Unless internal audit is serving as an internal consultant to build a BCP (as discussed in Chapter 28), internal audit generally is not involved in the project management processes for building the BCP. Its role comes later in assessing the adequacy of the completed BCP. An enterprise IT function, often in cooperation of key application owners, often is involved with launching a project for developing a BCP.

When reviewing an IT BCP, particularly a newly launched one, internal auditors should ask to see the project plans. Such plans should be created to build any BCP covering major applications. More important, an internal auditor should look for evidence of a risk assessment to determine why certain applications require full recovery treatment in the BCP.

To clarify things, normally the entire configuration of hardware and software should be set up for full recovery in a BCP program. However, for some lower-risk applications, it may not be necessary to restore all application transactions or processes immediately. Business continuity procedures refer to procedures that capture any active transactions that were in process during a system outage. In an airline reservations system, for example, BCP procedures should be designed to capture all transactions in process throughout the processing cycle. However, other files and processes may be fairly static, and there may not be a need to recover them immediately. A validation file that contains valid general ledger (G/L) account codes would be an example here. Such files generally are updated only periodically, and if a system failed at 3:00 A.M. on Tuesday, it would generally be sufficient to restore the G/L code file from a past update.

Exhibit 22.2 contains BCP plan review internal audit procedures for an internal audit review of a major or centralized data center review. While there are few common hardware and software configurations today, an internal auditor should look for evidence that IT management has considered business continuity risks on a major application-by-application basis and built a series of BCPs that cover those key applications. A major subset of a BCP for a centralized facility should be an emergency response plan. Such a plan allows the IT facility to react automatically in the event of an unexpected emergency, processes in an almost “fire drill” plans that. Emergency response plans do not promote business continuity. They are last-ditch efforts to abandon ship in the event of an emergency. Backup files and other procedures should be in place, but an immediate priority should be to preserve the health and safety of the IT personnel located at the centralized IT facility.

(ii) EMERGENCY RESPONSE PLAN OPERATIONS As part of any continuity planning review, internal auditors should attempt to gain assurance that appropriate emergency

EXHIBIT 22.2 Centralized IT Facilities Internal Audit BCP Review Procedures

1. Understand DRP Objectives and Status
   - Determine that IT and management understand the objectives of their DRP and expectations for recovery.
   - Review procedures for assessing risks and estimating costs with alternative DRP actions.
   - Understand the scope of the DRP, including equipment and processes covered and the scope of enterprise units.
   - Identify the equipment, floor plan, procedures, and other items necessary for the recovery.
2. Continuity Planning
   - Determine that the plan covers potential events, including weather, fire and flood, computer crime, and sabotage.
   - Determine that decisions have been implemented and arrangements made for backup processing facilities, whether a hot site or other facility.
   - Review risk assessments made, and their supporting analyses, to determine that the DRP coverage appears complete.
   - Determine that service-level agreement (SLAs) have been executed between applications users and key IT operations areas and that both understand their roles and responsibilities.
   - On a test basis, determine that backup processes are installed and working per DRP specifications.
3. Review Emergency Procedures
   - Review the emergency response plan, and, on a test basis, assess whether stakeholders are aware of the plan.
   - Review the results of the most recent two emergency response plan tests, and determine if it met expectations and the corrective actions were taken, if appropriate.
   - Assess whether current and appropriate contracts have been executed with DRP service providers, such a hot site facilities.
   - Assess whether communications have been established and action plans installed with outside providers, such as local fire and police facilities.
   - Determine that disaster recovery teams have been assigned and are aware of their responsibilities.
   - Determine that formal processes have been established for defining a disaster event and initiating the DRP.
4. Initiation of Recovery Procedures
   - Select several critical applications, and, on a test basis, determine that appropriate backups are being executed.
   - For those same critical applications, meet with key members of the business teams to determine that they understand their responsibilities for operating in a DRP environment.
   - Review the adequacy of processes for reviewing the DRP and keeping it current.
   - Review the DRP critical application testing programs, and assess their adequacy.
   - On a test basis, review the results of a critical process DRP test and determine that business operations have been restored adequately.
5. Maintaining the DRP
   - Assess the adequacy of processes in place to keep the DRP current, given different applications and technology changes.
   - Determine that procedures are in place to keep DRP documentation current, including communications with DRP providers.

procedures are in place to respond to and stabilize the situation following an incident or event. In the older days of IT, disaster recovery plans often were published in thick books located on the desks of a few key enterprise managers. The idea was that in the event of some emergency event, people would pull out the manuals to look up such data as the telephone number of the designated backup site to report the emergency or instructions for other emergency procedures. The material in these books might have worked if the manuals were kept up to date and the nature of the crisis event allowed time to review the manual and then react. Many real-life events are much more crisis oriented; there is little time to dig out the disaster recovery manual and read it. When the building is on fire, for example, people want to get out of the building as soon as possible, not spend time studying published evacuation instructions. Enterprises need to think through possible emergency situations, and internal auditors should review existing published materials with some skepticism.

Enterprises should establish emergency response plans with an emphasis on two significant types of emergency incidents. The first is a fire-in-the-building-type of incident; here the supporting emergency response plan would include posted fire exits and frequent fire drills. This type of emergency response plan should cover all enterprise operations, including IT resources, and should be tested regularly. A second level of emergency response plan should cover specific individual incidents that may or may not turn out to be significant but must be corrected at once, followed by an investigation and a plan of corrective action to prevent further incidents. These are called emergency *incidents,* and they often include such matters as security breaches or the theft of hardware or software. A good emergency incident response plan should be acted on quickly to minimize the effects of any further breaches. It should also be formulated to reduce any negative publicity and to focus attention on quick reaction time. The emergency incident response plan can be separated into four sections:

1. **Immediate response activities.** Whether the event is a security breach, a theft of assets, or physical intrusion, resources should be in place to investigate the matter and take immediate corrective action.
2. **Incident investigation.** All reported matters should be investigated fully to determine what caused the emergency and possible future corrective actions going forward.
3. **Correction or restoration.** Resources should be available to correct or restore things as necessary. Since emergency incidents can cover a wide variety of areas, these resources may include information systems security specialists, building security managers, or others.
4. **Emergency incident reporting.** The entire emergency incident and the actions subsequently taken should be documented along with an analysis of lessons learned and any further plans for corrective actions.

Emergency incident responses must be decisive and executed quickly. Internal auditors should assess established plans, recognizing that they should contain guidance to first act quickly and then only later build short-term strategies. Quick action is needed with little room for error. By staging practices like fire drills and measuring response times, response time speed and accuracy can be improved. Reacting quickly may minimize the impact of resource unavailability and the potential damage caused by any future systems or facility compromises. An enterprise faces

many potential emergency incidents or threats beyond a massive 9/11 type of emergency that causes the overall failure of IT resources. While the focus should always be on more major business continuity planning issues, an enterprise needs to have mechanisms in place to respond to every level of unexpected emergency event.

Looking for appropriate emergency response plans should be a component of many internal audit reviews. These plans will exist at a total facility level, such as a fire escape plan, or at an individual level, such as a plan to respond to a security breach. In many areas of the enterprise, auditors should ask if appropriate emergency response plans are in place, whether they are regularly updated and current, and whether they have been tested.

(b) Client-Server Continuity Planning Internal Audit Procedures

A client-server IT environment may contain multiple server systems covering applications, databases, and Web operations. These client-server environments are characteristic of smaller enterprises, where there is limited IT support for the enterprise but where IT systems are critical for ongoing business operations. These types of IT applications support such activities as distribution and billing for a smaller enterprise, or even a unit of a larger enterprise, but with a limited in-house IT staff. These types of critical applications are often installed by an outside provider tasked with establishing a BCP for key applications. However, all too often, such BCP efforts are never launched or, if they once were published, they quickly become out of date and are ignored.

The small- to medium-size enterprise that does not have an effective BCP for its IT operations faces a substantial risk. The Web is filled with testimony that reveals that a major IT failure at a smaller enterprise that lacks an effective BCP can easily force the enterprise to fail. The internal audit resources in such an enterprise often serve attempt to alert enterprise management to the risk of a key application failure and the need for effective BCP procedures.

The basic steps to build an effective BCP, no matter what the size of the enterprise, are essentially the same. A key activity is to back up, back up, and back up key files and applications. Internal audit can be a key resource to review existing BCP processes and to make appropriate internal control recommendations. Small- to medium-size enterprises often have not made arrangements for a formal hot site for its emergency backup processing, reasoning that the supporting hardware and software vendors can install replacement facilities in a short time.

Smaller system client-server environments often have fewer internal audit resources. However, as part of their general controls reviews of IT operations or of internal controls surrounding other operations, internal audit should be sensitive to the needs for an effective BCP. Although there are many variations here in terms of the size and business of the enterprise, Exhibit 22.3 is an internal audit readiness checklist for a client-server environment BCP. The idea here is that internal audit should survey and assess BCP readiness and make recommendations for improvements as appropriate.

(c) Continuity Planning for Desktop and Laptop Applications

Technology is constantly increasing the power and capabilities of desktop and laptop applications and systems. Small, handheld USB devices can plug into a laptop

EXHIBIT 22.3 Internal Audit Steps for a BCP Client-Server Readiness Review

1. Has a BRP been developed, approved, and tested for central or headquarters IT facilities?
2. Develop and document an understanding, from an internal audit perspective, of the enterprise's IT environment, including the identification of application, Web, and database servers as well as networks and Internet connections.
3. Based on an internal audit review, does the existing central DRP cover all supporting sever systems and networked facilities?
4. Is the environment multitiered with, for example, an application server linking to another nested operating environment? If so, determine that the existing DRP covers these extended resources.
5. Since a client-server environment typically depends on networked connections provided by communications vendors, has the DRP allowed for the failure of any of those elements?
6. Does the client-server appropriately link with any older legacy applications, and does the existing DRP cover that overall environment?
7. Where elements in the enterprise and the client-server environment are not included in the overall DRP, have provisions been made to include them?
8. Has a risk analysis been performed to identify the most critical applications, data repositories, and business functions?
9. Have interdependencies in the network been identified? For example, what would be the implications of the failure of a remote server in the operating environment?
10. Are backup processes in place for all key elements of the operating environment, and have efforts been made to coordinate those backups?
11. Is there a comprehensive DRP testing program in place covering all critical elements of the systems environment?
12. Does the DRP contain provisions for the potential loss of system elements—such as key server systems—in the ongoing recovery of the IT environment?
13. Does the DRP testing cover business operations as well as IT resources, and has internal audit been involved with observing critical portions of that testing?
14. On a test basis, determine that emergency response plans are in place and have been tested for critical elements of the network.
15. Is there an ongoing, enterprise-wide training program in place to inform all enterprise stakeholders of their DRP risks and responsibilities?

computer to provide sometimes 2 to 4 gigabytes[3] of memory. Although such devices are very cheap today, their size and capacity was almost unheard of not many years ago. Similarly, while desktop and laptop devices once had to be connected to larger systems through bulky cable arrangements, several different technologies allow the devices to be connected wirelessly.

Because of the power and flexibility of personal laptop and desktop devices, key managers in many enterprises have built critical files and other information repositories on these computers. These systems typically do not contain customer business transactions, but they often are repositories for other key enterprise documents, such as capital budgeting analyses, new product plans, and key product engineering data. An effective BCP is just as important, if not more so, for these data files than for the supporting databases for business applications. These personal systems, particularly the laptop devices, on which control often is limited to the system's owner, can raise BCP concerns and certainly cause potential security risks.

EXHIBIT 22.4 Desktop and Laptop Systems BCP Processes

1. Does the enterprise restrict business data and applications to company-controlled devices?
2. Are inventory records maintained regarding the number of desktop and laptop systems in use, their owners, and the application activities?
3. Are enterprise policies in place restricting or limiting the use of desktop or laptop devices for sensitive data?
4. Has the enterprise-wide BCP considered organization IT risks and resources located on desktop or laptop devices?
5. Are there enterprise-wide procedures in place that require employees to download their key files and programs to remote storage devices?
6. Where such backup procedures are in place, are associates following these system download and backup rules? Assess this functionality by reviews of procedures on a test basis.
7. Are there active training programs in place to inform desktop and laptop system users of the risks of data loss?
8. On a test basis, determine that the business operations from the backup storage files system can be restored to replacement systems for continued business operations.
9. Along with desktop and laptop system BCP processes, has proper attention given to systems security and integrity concerns?
10. Are there processes in place to integrate and coordinate desktop and laptop processes with normal enterprise process resources?

Internal auditors should be aware of the BCP risks surrounding laptop devices in particular. Today's internal auditors are using laptop audit computers to record the results, store test results, and carry many other audit report–related data. While the internal audit department should have strong procedures regularly requiring internal auditors to back up their work to a centralized location, an incident such as a stolen or damaged audit computer—even with appropriate backup resources—can impact internal audit progress and even represent a security breach. Just as an internal audit function should have strong procedures for the backup and retention of work on single desktop and laptop devices, an enterprise should have some strong enterprise-wide backup and BCP procedures for all stakeholders using laptops and other portable devices. Exhibit 22.4 outlines some BCP best practices for desktop and laptop personal computer systems.

22.3 Building the IT Business Continuity Plan

As mentioned earlier, what were once called disaster recovery plans were often published in thick notebooks that became out of date almost as soon as they were published and distributed. In addition, they focused on recovering IT operations from a disaster event but not primarily on recovering the business and its key operations. Many enterprises have established some form of disaster recovery plan for good business and internal control reasons. Those enterprises that established such plans following those old rules probably do not have effective BCPs in place today.

This section outlines steps to build an effective BCP for an enterprise. Internal auditors often can play a key role in this process with their knowledge of business systems of and the internal control requirements of the Committee of Sponsoring

Organizations (COSO) internal controls framework or the *C*ontrol *ob*jectives for *i*nformation and related *T*echnology (CobIT) frameworks, as outlined in Chapters 3 and 5. Although the words *disaster recovery* and *BCP* are not found specifically in the SOx legislation, the astute board audit committee or chief financial officer should realize that an enterprise must have an effective BCP in place and working both in order to attest that the internal controls are effective as required in SOx Section 404 and to release its financial results in a timely manner.

If an enterprise already has an existing BCP for part or all of its business activities, it needs to be reviewed to determine whether it can meet projected business continuity needs effectively—and we emphasize the business recovery aspect of the plan here. All too often, some enterprises have just renamed their old-style disaster recovery plans with minimal thought to business continuity requirements. The BCP should be current or regularly updated. It should have a detailed section on incident and risk assessment covering all key business activities and include a strategy for recovery of all significant business processes, including applications, communications resources, and other IT assets. There should be assignments for disaster and business teams as discussed in Section 22.3(c). The BCP should contain detailed instructions for the business recovery process, including overall project enterprise notification and reporting procedures. Once any existing BCP is reviewed and assessed for adequacy, it should be enhanced and updated as required.

If no BCP exists or if the current version is very much in need of help, a project should be launched to create a new BCP with a designated project manager appointed to lead the effort. This individual should have good leadership qualities, an understanding of business processes, skills with IT security management, and strong project management capabilities. An ideal candidate might have Project Manager Professional (PMP) credentials.[4] For some enterprises, the information security officer may be an ideal candidate for this role. In other cases, internal auditors may be requested to act as internal consultants. The objectives and deliverables for such a BCP project need to be clearly defined to enable the overall BCP project team to ensure that their work is consistent with original project expectations.

A BCP project's principle objective should be for the development and testing of a well-structured and coherent plan that will enable the enterprise to recover normal business operations as quickly and effectively as possible from any unforeseen disaster or emergency that interrupts normal IT services. Subobjectives should ensure that all employees fully understand their duties in implementing the BCP, that information security policies are adhered to within all planned activities, and that the proposed business continuity arrangements are cost effective. The BCP deliverables should consist of:

- Business risk and impact analysis
- Documented activities necessary to prepare the enterprise for various possible emergencies
- Detailed activities for initially dealing with a disaster event
- Procedures for managing the business recovery processes, including testing plans
- Plans for BCP training at multiple levels in the enterprise
- Procedures for keeping the BCP up to date

Each of these major BCP components is discussed in next sections. A major objective here is to allow the enterprise to restore business operations as quickly and effectively as possible after a disaster event. This activity requires active participation on many levels. Internal auditors should understand these BCP processes in order to make appropriate recommendations for improving the effectiveness of an enterprise's BCP.

(a) Risks, Business Impact Analysis, and the Impact of Potential Emergencies

Risk analysis, as discussed in Chapter 15, is an important BCP analysis tool. Risk or business impact analysis is particularly important for determining what applications and processes to include in the overall BCP. In the past, recovery analysts and sometimes internal auditors focused too much on the subjective probabilities of some event occurring. That is, there were extensive discussions covering the potential probability of a tornado, an earthquake, or some other catastrophic event at a data center location. Those analyses focused on the loss of a centralized data center but not on the continuity and recovery of business applications.

Today's BCP should include a descriptive list of the enterprise's key business areas, typically ranked in order of importance to the business, as well as a brief description of the business process and its main dependencies on systems, communications, personnel, and data. If the enterprise already has prepared an assessment of its key business processes, the BCP team can update that documentation and evaluate the relative importance of each process. It should be emphasized that this is an inventory of *business processes,* not critical IT application systems. While the two are often one and the same, it is important that they be considered as the key processes necessary to keep the business operating.

A next step here is to look at those key business processes in terms of potential business process outage failure impacts. Exhibit 22.5 shows a business impact outage impact analysis in an Excel worksheet. Each separate key business process would be listed in the column on the left with risk of failure factors considered for each key business process such factors as the Impact on Customer Services, Loss or Customers, and the like. The idea here is to use this schedule to analyze the time-based relative risks of various categories of exposures in the event of a business outage. Within each of these risk factors, the impact or criticality of various levels of outages should be considered. Various factors, such as a specified application failure of less than two hours that will impact customer services but will cause a minimal loss of customers and essentially no risk of exposure to possible litigation, can be described on the chart.

While monetary values can be added to the schedule shown in Exhibit 22.5, this can be equally effective as just a worksheet to highlight key time-based exposures. This type of outage analysis table and the steps necessary to get back in operation are key components of what is usually called a business impact analysis (BIA). A newer term in the world of disaster recovery and business continuity planning, BIA is the process of defining the key business process risks that will impact business operations as a result of a loss of services.

This type of schedule can help an enterprise look at all of its significant enterprise applications or processes and assess their time-based failure impacts. For example, under the Possible Litigation columns, each key application would be assessed when

Business Process	Customer Service Failures						Loss of Customers						Loss of Business Revenue						Penalty Clause Exposures						Possible Litigation						Loss of Key Information					
	< 2 hr	2–24 hr	24–48 hr	2–5 days	> 6 days		< 2 hr	2–24 hr	24–48 hr	2–5 days	> 6 days		< 2 hr	2–24 hr	24–48 hr	2–5 days	> 6 days		< 2 hr	2–24 hr	24–48 hr	2–5 days	> 6 days		< 2 hr	2–24 hrs	24–48 hr	2–5 days	> 6 days		< 2 hr	2–24 hr	24–48 hr	2–5 days	> 6 days

Note: This schedule is used to analyze risks by key business processes of the impact of various types of failures. For example, what is the relative risk of loss of customers if the process is out less than 2 hours, 2 to 24, etc.?

EXHIBIT 22.5 Business Criticality Outage Impact Analysis

there might be a risk of litigation to the enterprise if a given application were down two hours or more.

Based on the outage risks, the BCP team would study and document its recovery requirements for their key business processes: business process procedures, automated systems, and hardware plus software requirements. In addition, the team should reevaluate any existing backup and recovery procedures. In larger enterprises, BCP-like arrangements are sometimes made by individual business units that may not be consistent with overall enterprise-wide BCP arrangements. Again, the emphasis here should be on recovering business operations, not just on getting the automated systems operating again.

(b) Preparing for Possible Contingencies

Once the BCP project team has reviewed business processes, completed its initial processes, and assessed the business risks, next step should be to minimize the effects of potential emergencies. An objective here is to identify ways of preventing an emergency situation from turning into an even more severe disaster for the enterprise due to the lack of preparedness. The BCP project team should focus on activities that are essential to the continued viability of the business and should develop appropriate backup and recovery procedures for the identified critical applications. The complexity and cost of these backup business continuity procedures will depend on the identified business process restoration needs.

Internal audit should consider a review of the enterprise's BCP, since such a review will almost always score high on any risk criticality planning exercise. There are many variations on how a BCP might be constructed as well as variations of overall enterprise risk; Exhibit 22.6 outlines some general review points for a BCP audit. It discusses some areas that internal audit should consider in order to discuss the effectiveness of the plan with the audit committee.

Enterprises have a variety of options for establishing a backup strategy. Larger enterprises often have the resources to do much of this on their own, although many rely on outside vendors to provide backup processing services. An enterprise generally commits to one of these strategies:

- **Fully mirrored recovery operations.** This approach requires building what is called a fully mirrored duplicate site with linkages between the live site and the backup, mirrored alternate facility. However, specialized storage management hardware and software is almost always the most expensive option. Fully mirrored strategies provide the greatest level of recovery assurance.
- **Switchable hot site facility.** Here arrangements are made with a vendor that will guarantee to maintain an identical site with communications to enable the transfer of all data processing operations to this site within an agreed time period, usually less than one to two hours. Because of the need to keep the equivalent of an exact duplicate site in waiting, the costs here can be almost as high as a fully mirrored arrangement.
- **Traditional hot site.** Here the enterprise contracts with a disaster recovery vendor with a compatible site to enable the switching of IT operations to that site within an agreed time period, usually less than eight hours after notification. This very common recovery approach became very much challenged after 9/11. Too

EXHIBIT 22.6 Internal Audit Review Points for a BCP Audit

1. Plan and schedule the review following internal audit's planning risk assessment approaches.
   1.1. Review the results of any past internal audit BCP review, noting audit findings and corrective action plans.
   1.2. Determine the scope of the BCP review: specific business units or enterprise-wide.
   1.3. Schedule staff to initiate the internal audit.
2. Review the existing BCP with the responsible manager.
   2.1. Does the BCP appear to be current and up to date?
   2.2. Does the BCP cover all areas of the enterprise, including business processes, or just primarily IT operations?
   2.3. Are there open BCP issues to be resolved?
   2.4. Has the BCP been reviewed with key members of management, and do they appear to understand their responsibilities under the BCP?
   2.5. Has internal audit's BCP review plan been reviewed with the audit committee?
3. Examine the contents and format of the BCP.
   3.1. Based on internal audit's understanding of enterprise operations, does the BCP appear to cover key business processes and their supporting IT tools?
   3.2. Does the BCP documentation include adequate levels of business impact analysis and risk assessments?
   3.3. Does the plan appear to cover appropriate procedures for backups—such as the use of mirroring—and off-site storage?
   3.4. Does the BCP contain step-by-step outlined procedures for execution in the event of an emergency?
   3.5. Does the BCP include call list chains?
   3.6. Does the BCP include key vendor and emergency supply contacts?
   3.7. Does the BCP document contacts for fire, police, and external media?
   3.8. Is there a process in place to provide for regular and automatic updates of the BCP?
4. Analyze the business and IT service-level agreements (SLAs) covering BCP activities.
   4.1. Determine that the enterprise has established appropriate SLAs covering the BCP.
   4.2. Interview several interested parties to assess that they understand their BCP roles and responsibilities.
5. Analyze overall training and understanding of the BCP.
   5.1. Discuss the BCP with several members of the team designated to execute the plan to determine their understanding.
   5.2. Do members in IT operations and systems appear to understand their roles and responsibilities?
   5.3. Based on discussions with key persons in critical business process areas, does there appear to be a general understanding of their business recovery roles?
   5.4. Based on an interview with the CFO or designee, is there adequate understanding of the BCP and how it will operate?
   5.5. Based on review of the BCP training records, does training appear to be adequate, timely, and regularly scheduled?
6. Review the results of recent BCP tests.
   6.1. Is there a formal program of testing critical BCP elements?
   6.2. Are testing results documented in a lessons-learned format?
   6.3. Does BCP testing cover both business recovery as well as IT functions?
7. Review BCP backup procedures.
   7.1. If a remote hot site vendor is used, review the contract and related documentation for currency.
   7.2. Review the documented results of hot sites tests.
   7.3. Review the adequacy if other backup vendor or location procedures.
8. Prepare internal audit documentation assessing the overall adequacy of the enterprise's BCP.

many enterprises in distress contacted the same hot site vendors, which did not expect to have to support many disaster events simultaneously.

- **Cold site facility.** This is a more frequent approach when disaster recovery sites are viewed as very expensive and enterprise IT management wants some possible solution. The strategy involves establishing an emergency site to allow the enterprise to begin processing as well as a standby arrangement with vendors to deliver minimum hardware configuration. This strategy goes back to the days when mainframe computers required air conditioning and water cooling operations that were located under raised-floor computer room sites. In theory, those cold sites could be operational within two to three days.
- **Relocate and restore.** This is the weakest level of backup strategy. It involves the identification of a suitable location, hardware and peripherals, and the reinstallation of systems and backed-up software and data *after* an emergency has occurred. Some managers have been guilty of advocating this approach. They have backed up their software and data with no firm plans beyond just making arrangements if something happens. This strategy is inadequate for today's business processes.
- **No strategy.** Almost unheard-of today, some enterprises still have no backup and restore strategy for their IT resources and operations This is often an "I'll get to building my BCP later, I'm too busy right now!" type of approach. This approach carries the highest risk of all. In the event of a disaster, this strategy usually ends up with the enterprise going out of business. The internal auditor who encounters this situation should make this a strong business risks warning to the audit committee.

An enterprise BCP must contain appropriate strategy for the backup and recovery of an enterprise's IT and for business continuity. These BCP procedures, especially for key business processes, should be designed to get business operations back in operation per management requirements. While in some instances a decision to use a hot site strategy will be the major direction for almost all applications, some highly critical process may require full mirroring capabilities. Such a mixed mode of backup strategies can be appropriate if the enterprise decides that full mirroring is justified only for that one highly critical process while the others will rely on an adequate but appropriate hot site strategy.

No matter the approach selected, all key processes in an enterprise should have some level of backup and restoration policy that allows the overall business to remain in operation. While not all processes may require full mirroring, for example, all should be part of a consistent, comprehensive approach that will allow the overall business to get back in operation in the event of a serious disruption. The cost of recovery can be a major factor here, and the BCP team should outline cost options and get the application owners to buy in to an option through appropriate agreements. Internal audit, in its periodic reviews of BCP procedures throughout the enterprise, should highlight any discrepancies encountered here.

The BCP should have a high-priority objective to provide an adequate level of service to all customers throughout an emergency. Critical customer service activities should be included in the BCP, ordered in a priority sequence with restoration steps outlined in some level of detail. Business managers who understand customer needs may not be part of the recovery site BCP team, particularly if it would be operating at a remote hot site. Documentation describing key customers and customer service

activities should be essential components of the BCP. The emphasis should be on getting the enterprise back in operation.

No matter what backup strategy is used, key files and documents should always be stored in secure off-site locations. Disaster recovery and business recovery teams should be designated and trained, with periodic tests to assure their ongoing familiarity with processes.

(c) Disaster Recovery: Handling the Emergency

Building a BCP is a relatively easy process when the team sits in a closed room, brainstorms, talks through, and plots a business continuity recovery strategy. It suddenly becomes more difficult when alarm bells ring signifying that an emergency event has occurred, and the enterprise needs to enact all or some portion of the BCP. As a first task, the enterprise must determine the level to which the emergency situation requires activation, including the full BCP and notification of the emergency response team. This notification usually should be communicated in a preagreed call list–driven format with members of the disaster recovery team instructed to assemble at a designated off-site location. In addition, management and key employees should be kept informed of developments affecting the BCP activation and its impact on their areas of responsibility. The BCP project team leader would be responsible for this notification activity.

The objective of this BCP phase is to get back in operation. This almost always involves contacting the designated alternate processing site, activating communications lines, making arrangements to get the team to that site, and otherwise taking steps to restore operations. Assuming the team is using a hot site vendor, the disaster recovery team should arrive at a backup site, get operating systems versions and key databases loaded, and begin production operations. These steps are often far easier said than done, and it is sometimes a challenge to get communications lines connected and up and running in the new environment. This process must be handled in a short time frame with the objective of having as many critical business processes as possible restored and operating quickly.

For the BCP and its recovery process to be effective, the recovery team must carefully consider and plan for the potentially complex series of activities needed to recover from a serious emergency. A planned approach is likely to result in a more coherent and structured recovery. It is likely that a serious disruptive event will produce unexpected results that may differ in some ways from the predicted outcomes contained within this plan. The recovery team should review any predefined procedures or strategies in light of the actual situation arising after the emergency event and modify these procedures as appropriate.

(d) Business Continuity Plan Enterprise Training

As discussed previously, extensive BCP processes and published documents are of little value unless the people responsible for executing them are trained regularly in their use. Many traditional disaster recovery plans were not very practical in a 9/11 type of disaster, where entire buildings suddenly collapsed. Secure, online plans will provide some help here, but what is needed is a BCP team familiar with the emergency response plans discussed earlier and trained in the general processes necessary in the event of an extreme emergency. Certain BCP team members must

know enough about the plan so they will react almost instinctively in the event of a severe emergency situation.

In order for people to act without having to flip through a published plan to decide the next step, members of the enterprise must be trained. The BCP project team should launch a business continuity planning training program. These four levels of BCP training are suggested:

Level 1: General management overview. Training should be given to a wide range of people, starting with the audit committee, to outline the overall strategy for recovery in the event of an emergency event and to describe expectations of how the enterprise would operate in a business continuity environment.

Level 2: Key application systems users. Training here should be focused on recovery procedures for critical applications. In many instances, critical applications should function in a business-as-usual sense except that processing will take place at the alternate hot site. However, some normal resources, such as user help desks, often will not work in the same manner. This training should be oriented to designated critical applications and how they are planned to operate and should operate in a case analysis mode. Here users can review BCP processes for their applications and ask detailed questions or point out areas where corrective action may be needed.

Level 3: IT operations and systems staffs. The IT staff, including those with both infrastructure operations and systems responsibilities, are usually those who will be most impacted by a business continuity event. Training here should emphasize and reemphasize key elements of the BCP; it should take the format of regular and periodic fire drills. In some instances, this training can be based on actual BCP tests. In others, game-type simulations may be effective.

Level 4: BCP team members. The team that built and launched the BCP should have the greatest familiarity with established BCP procedures. Nevertheless, their knowledge needs to be refreshed and updated on an ongoing basis.

An effective training program is a final step to building an effective and enterprise-wide BCP. While internal auditors, in their normal assurance level of activities, typically will not be leading an enterprise project to build and launch an enterprise BCP, often they will be very involved in its development and practices. In addition, they should include the status of continuity planning in the regular audits of both IT operations and other business areas.

22.4 Business Continuity Planning and Service-Level Agreements

An enterprise and its IT function cannot just arbitrarily publish and release a BCP for its business process and application areas. There must be a strong buy-in from the application owners as well as a joint understanding of expectations and service delivery. If a senior executive in a specific user department feels that some of her business processes must *always* be operational with a full backup capability, that department should negotiate with IT to provide that level of business continuity service; the department also must recognize the necessary costs of additional

hardware and software to provide that capability. In the past days of downloaded backup tape copies periodically shipped to a remote location, anything close to an immediate backup was only theoretical. A transaction had to be written first in the main system and its database and then copied to a backup facility. There was always a delay, ranging from weekly or daily backup files to almost immediate real-time system approaches. Newer mirroring storage management approaches today can provide immediate backups. Described in the next sections, these techniques are very effective but certainly more expensive.

In order to make a BCP work between IT and business units, they should jointly negotiate their recovery expectations through formal service- level agreements (SLAs). A SLA is a contract between the business process owner and the provider of IT services for specified service objectives. SLAs are discussed as part of the information technology infrastructure library (ITIL) service delivery best practices in Chapter 18 and are fundamental to business continuity activities. An example of an SLA is shown in Exhibit 18.8. Internal auditors should be aware of the importance of SLAs and should look for effective SLA implementations. A SLA is effectively a contract between IT and key user areas to support both normal day-to-day operations as well as the actions to be taken in the event of a serious service disruption. SLAs describe expected and promised levels of business continuity services and are basic building blocks for establishing effective BCPs.

All IT organizations should establish internal SLAs, but they are found most frequently in the contracts for the services of outside IT providers. For example, an IT services vendor may agree to handle the processing of some application at a rate of x cents per transaction and may also agree to process these transactions within a specified turnaround time. The enterprise pays for these services based on the transaction rate and recognizes adjustments if expected turnaround time standards are missed. Similar SLA arrangements between users of services and IT should be made within the enterprise, but the internal costs usually are based on internal budget amounts. For a BCP-related SLA, the benefitting user business function will specify its backup needs and will accept a periodic budget charge for those information systems and related services. If promised SLA targets are missed, a budget credit would be issued. Even though these SLA debit and credit amounts often are based on internal "funny money" transactions, they can become an important measure of management performance.

Business recovery SLAs frequently are structured to cover most if not all departments or functions in the enterprise. SLAs describe an IT function's commitment or promise to provide an agreed on level of business continuity services. When a business area has specific needs, special or unique SLAs should be created. Internal auditors should be aware of the importance of SLAs when reviewing business continuity planning and the enterprise's BCP. As mentioned, Chapter 18 has more information on building and launching SLAs. This is the type of contract that sets appropriate rules and expectations.

22.5 Newer Business Continuity Plan Technologies: Data Mirroring Techniques

When reviewing systems or applications controls, internal auditors usually ask whether key files are backed up on a regular basis. However, many systems backup procedures to download copies of critical transactions are not effective in today's

world of constant streams of real-time transactions. Full file or database backups taken every week, every day, or even every hour along with captured streams of interim transactions are just not effective in our world of constantly updated applications. When a system shuts down because of some emergency, it is necessary to go back to the most recent database backup as a benchmark or starting point and then reprocess all transactions submitted after the last backup to the present. However, when the business process is very active, such as for high-volume trading or ordering, it is almost impossible to get caught up reprocessing past transactions without shutting down the actual application. An airline ticketing and scheduling system is an example. In order for the enterprise to survive, the system must be operational virtually at all times around the clock and at a high-level availability rate. For an enterprise to state that it is operating and available nearly 100% or 99.99% of available time, it can be out of operation less than one hour per year. Exhibit 22.7 outlines these high-availability percentages, and many modern enterprises seek to assure themselves and their stakeholders that they are nearly 100% available.

Legal and regulatory mandates for business continuity make this high availability a top priority, and an enterprise needs to move and copy its data in order to recover critical business operations rapidly in the event of data loss, data corruption, or disaster. Many new technology advancements over recent years allow rapid and frequent backups. A technology known as RAID (Rapid Array of Independent Disks), for example, is often used; data are copied simultaneously to multiple locations on one or more disk files to create redundancy. We encounter RAID at a very basic level on a desktop computer using Microsoft's XP operating systems where, if a power failure or the like, a restored version of disk files is retained. While of no help in a total disk crash, this technology provides perhaps the most efficient level of backup and recovery for desktop computer systems.

Perhaps the most efficient backup strategy today is through what is called mirroring. Mirroring is just what the name implies. If we set two glass mirrors on the table in front of us at 45-degree angles, when looking at them, we will see two images of ourselves at once. Mirroring data achieve the same results. Pressing the enter key for a computer transaction immediately writes it to three devices, the original and the mirrors. This process involves establishing a "shadow" disk that is updated in parallel with the primary disk, providing a real-time or near-real-time copy of the primary disk. Local mirroring provides the first level of data protection with a mirror disk attached to another system at another site, often through an Internet connection. In the event of data loss on the primary disk, the data can be retrieved seamlessly from the mirror disk. The process of mirroring distinguished itself during the 9/11 terrorist attack. Systems where mirroring was installed essentially lost no computer data when the twin towers were destroyed. Businesses resumed operations at remote sites as soon as they were able to get to those sites, but with essentially no loss of data.

EXHIBIT 22.7 High-Availability Percentages

Availability	Number of Decimal 9s	Estimated Down Time per Year
99%	Two 9s	87 hours
99.9%	Three 9s	8 hours
99.99%	Four 9s	52 minutes
99.999%	Five 9s	5 minutes
99.9999%	Six 9s	Less than 1 minute

Mirroring is a newer and evolving method for data backup retrieval today. Internal auditors certainly do not need to become experts on the application or use of backup retrieval methods. More important, an internal auditor should be generally aware that such instant backup procedures are available and can be installed to promote business continuity.

22.6 Auditing Business Continuity Plans

Internal audit can and should play an important role in an enterprise's BCP development as well as its testing processes. Internal audit might offer its resources to observe and comment on the results of BCP tests, to suggest testing scenarios, or to offer consultative advice on the progress of the BCP development. While internal audit can be part of these BCP processes, it should step back periodically, assert its independence, and schedule periodic audits regarding the adequacy of BCP processes and business recovery procedures in general. Audits should be planned and scheduled as part of internal audit's regular risk assessment and audit planning process.

While internal audit may play the role of observers in the BCP testing process, formal internal audits should be scheduled periodically to assess all aspects of BCP readiness and the adequacy processes in place. Internal audit must be careful of the fine line between acting as an advisor or consultant to the BCP team and auditing its processes. Internal audit's review of enterprise BCP processes should be based on such matters as the adequacy and currency of its BCP documentation, the results of scheduled tests, and a host of other issues. While every enterprise is different, an internal audit review should focus on an audit of one self-contained set of resources and processes but can be expanded for a larger, multilocation enterprise.

An adequate business continuity process is an important component of an enterprise's internal control structure, as was discussed in Chapters 3 and 4. Internal audit should communicate the results of its reviews here with senior enterprise management as well as the audit committee. The results of the BCP audit should be included in the internal materials that would be part of the enterprise's Section 404 assessment of internal controls.

22.7 Business Continuity Planning Going Forward

As enterprises become ever more dependent on their automated business systems, procedures to keep those processes in operation after an emergency or disaster have become increasingly important. The enterprise's staff can no longer get by with pulling out their No. 2 pencils and completing paper forms as backup processes. Our automated systems are tied to complex in-house and Internet-based databases; those old procedures are no longer applicable. Going forward, the 2001 terrorist event proved that many older business continuity procedures were just not applicable. The mirroring processes discussed in this chapter point to a direction for business continuity planning.

The old "disaster recovery" rules have changed as well. It is no longer sufficient for IT operations to move to a hot site backup location to begin processing and assume the enterprise will soon be up and running. Processes must focus on restoring

business operations in light of an extended interruption in IT services. Businesses need the ability to get all processes back in operation with minimal delay. Internal auditors have an important role here in helping management to implement effective BCP processes and in regularly assessing their operations and controls. Although there can be many variations and approaches to an effective implementation, all internal auditors should have at least a general knowledge of BCP requirements and how to assess such a process. In today's highly automated world, an understanding of BCP requirements and best practices should be part of an internal auditor's CBOK.

Notes

1. Disaster Recovery Institute International, Falls Church, VA (www.dri.org).
2. "Technology on the Web," *Forbes*, March 29, 2004.
3. Gigabyte, abbreviated GB, refers to a unit of computer storage meaning either exactly 1 billion character unit bytes (1000^3, or 10^9) or approximately 1.07 billion bytes (1024^3, or 2^{30}).
4. PMP is an examination- and experience-based qualification administered by the Project Management Institute (www.omi.org).

PART VI

Internal Audit and Enterprise Governance

CHAPTER 23

Board Audit Committee Communications

Other chapters have talked about how to manage many internal audit processes or how to enhance internal audit procedures. Internal audit's relationship with the board of director's audit committee presents a different challenge to all members of the internal audit team. Internal audit reports to the audit committee, which approves its overall planning activities and reviews the results of internal audits. However, the relationship here is often a bit different from a classic supervisor–subordinate relationship. Audit committees have become much more active in their oversight of internal audit activities since the launch of Sarbanes-Oxley (SOx), but usually the committees are not physically present on a day-to-day basis. Internal audit's chief audit executive (CAE) is often the main contact with the audit committee and frequently must educate and advise the committee on internal auditing issues. For many corporations today, the audit committee's relationship with internal auditors is an evolving issue. Many audit committees understand the financial reporting issues associated with their external auditors but sometimes view internal audit as an almost unfamiliar resource.

This chapter reviews the role of today's audit committee and its responsibilities for internal audit. We discuss the committee's roles in approving the audit charter, appointing the CAE, approving audit plans, and reviewing the results of internal audits. The chapter also discusses the types of reporting that internal audit should supply the audit committee to present the results of their work and to highlight issues that may require further action. SOx has mandated other audit committee responsibilities, such as a role in managing a financial violation whistleblower program. This role is discussed further in Chapter 24; here we discuss how internal audit can aid the audit committee in such initiatives.

The audit committee has the responsibility to set the overall direction for internal audit. While many members of internal audit often may not have much day-to-day contact with the audit committee members, everyone there must realize that the audit committee is the final source to report matters of unusual concern and to seek resolutions. All internal auditors should have a common body of knowledge (CBOK) high-level understanding of the role and responsibility of the audit committee in today's enterprise.

23.1 Role of the Audit Committee

A significant step in initially organizing an internal audit function in a new enterprise is to obtain authorization and approval by the enterprise's audit committee of the board of directors. The audit committee provides this broad authorization for an internal audit function through the formal audit charter document that was discussed in Chapter 12. An audit committee also approves internal audit's overall plans for continuing activities through the current period and beyond. As one of the several operating committees established by the board, the audit committee has a unique role compared to other board committees. It consists of only outside directors—giving it independence from enterprise management—and should be composed of outside directors who generally understand, monitor, coordinate, and interpret the internal control and related financial activities for the entire board. As discussed in Chapter 4, one of those audit committee members must be designated as a financial expert per SOx rules. In order to fulfill its responsibilities to the overall board of directors, to the stockholders, and to the public, an audit committee needs to launch and manage an internal audit function that should become an independent set of eyes and ears inside of the enterprise, providing assessments of internal controls and other matters.

The comments in this chapter are based on a corporate structure such as one with Securities and Exchange Commissions (SEC) registered stock. Other nonpublic enterprises will benefit from an audit committee structure as well. For example, many not-for-profit or private enterprises are large enough to have a formal board of directors and an internal audit function. Although not mandated to do so by SOx and SEC rules, such organizations will benefit from a board audit committee of only independent directors. An internal auditor in such enterprises would benefit both the internal audit function and the overall enterprise management by suggesting this type of approach.

While external auditors have a prime responsibility to an enterprise's board of directors for attesting to the accuracy and fairness of financial statements, internal audit has an even larger role in assessing internal controls over the reliability of financial reporting, the effectiveness and efficiency of operations, and the enterprise's compliance with applicable laws and regulations. Corporate boards of directors have had formal audit committees for some time, and internal audit has always had a long-term reporting relationship to the board of directors' audit committee. However, much has changed since SOx in mid-2002. In past years, many audit committees met only quarterly for brief sessions in conjunction with regular board meetings; those meetings often were limited to little more than approving the external auditor's annual plan and their quarterly and year-end reports and reviewing internal audit activities in what appeared to be little more than a perfunctory basis. While New York Stock Exchange (NYSE) rules, even prior to SOx, required that audit committees consist of only outside directors, in the past many audit committee directors often appeared to be buddies of the chief executive officer (CEO) with apparently little evidence of true independent actions. Internal audit's CAE has always had a direct reporting relationship to the audit committee, but often this was little more than a theoretical relationship where the CAE had limited contact with the audit committee beyond scheduled board meetings. SOx has now changed all of that.

During the first years of this century, a major issue that evolved from the collapse of Enron and the related financial scandals was the fact that boards and their

audit committees were not exercising a sufficient level of independent corporate governance. The Enron audit committee was highlighted as an example of what was wrong. It was reported to have met some 30 minutes per calendar quarter prior to the company's fall. Given the size of Enron at that time and the many directions it was pursuing, the audit committee's attention appeared to be limited at best.

Even before the fall of Enron, the SEC was becoming interested in seeing audit committees acting as more independent, effective managers of a company's external and internal auditors. For example, in 1999 the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees was formed by the NYSE, SEC, American Institute of Certified Public Accountants (AICPA), and others. It issued a series of recommendations on improving the independence, operations, and effectiveness of audit committees. The stock exchanges then adopted new independent director audit committee standards as listing requirements to be phased in over the next 18 months, and the Auditing Standards Board of the AICPA raised standards for external auditors with respect to their audit committees. The subsequent financial failures of Enron and others showed these initiatives were not enough. The result was the legislative work that led to SOx.

Today, since the passage of SOx, audit committees have expanded responsibilities and internal audit has a greater responsibility to best serve its audit committee. Although an audit committee typically has regular contacts primarily with the CAE, all internal auditors should have an understanding of this very important relationship. We discuss heightened audit committee responsibilities and how internal audit can better work with an audit committee under SOx rules.

23.2 Audit Committee Organization and Charters

An audit committee is an operating component of the board of directors with responsibility for internal controls and financial reporting oversight. Because of this oversight responsibility, audit committee members must be independent directors with no connection to enterprise management. There are no size restrictions, but a full board with 12 to 16 members will often have a 5- or 6-member audit committee. An audit committee may invite members of management or others to attend committee meetings and even to join in on the deliberations. However, any such invited outside guests cannot be full voting members. An enterprise's board of directors is a formal entity given the responsibility for the overall governance of that enterprise for its owner investors or lenders. Because all members of the board can be held legally liable through their actions on any issue, and a board and its committees enact most of its formal business through resolutions, which become matters of enterprise record. The enterprise of the board's various committees, including the audit committee, is established through such a resolution. Exhibit 23.1 is a sample board resolution to establish an audit committee. This type of resolution is documented in the records of the board and not generally revised unless some circumstances require a change.

Exhibit 23.1 is an example company board resolution authorizing their audit committee; it is an example of the way in which a board of directors sets rules for itself. Such resolutions are an example of corporate governance setting the rules by which a corporation operates. While not published in annual reports and the like, the existence of appropriate board resolutions becomes issues in matters of regulation

EXHIBIT 23.1 Board Resolution Example: Authorizing the Audit Committee

ExampleCo Corp Board of Directors

Board Resolution No. XX, MM, DD, 20YY

The Board of Directors authorizes an audit committee to consist of five directors who are not officers of ExampleCo. The Board will designate one member of the Audit Committee as a Financial Expert, per the requirements of the Sarbanes-Oxley Act, and elect one member to serve as its chair for a term of three years. The ExampleCo Chief Executive Officer may attend Audit Committee meetings as a nonvoting member at the invitation of the Audit Committee.

The ExampleCo Audit Committee is responsible for:

- Determining that ExampleCo internal controls are effective and formally reporting on the status of those controls on an annual basis with quarterly updates.
- Recommending an external auditor to be selected on an annual basis through a vote by the shareholders.
- Taking action, where appropriate, on significant control weaknesses reported by internal audit, the external auditors, and others.
- Approving an annual plan and budget submitted by the external auditor.
- Approving annual audit plans to be submitted by the outside auditor as well as by internal audit.
- Approving the appointment and ongoing service of Internal Audit's Chief Audit Executive.
- Approving the annual internal audit plan and recommending areas for additional internal audit work as appropriate.
- Reviewing and distributing the audited financial statements submitted by the outside auditor.
- Establishing an ExampleCo whistleblower program that allows officers, employees, and other stakeholders to report financial accounting errors or improper actions and to investigate and resolve those whistleblower calls without any retribution to the original whistleblower.
- Circulating a Code of Ethics to senior officers and obtaining their assent on a quarterly basis.
- Initiating appropriate actions based on any recommendations by the outside auditor or the Director of Internal Audit.
- Maintaining records on other consulting activities as mandated by the Sarbanes-Oxley Act.

An Audit Committee meeting will be held at least concurrently with each scheduled Board meeting and at other times as required.

The Audit Committee will meet privately with the outside auditor or the Chief Audit Executive to assess the overall internal control environment and to evaluate the independence of the audit function.

Approved: Corporate Secretary

and litigation only when a board needs to rely on an authorizing resolution. After SOx first became U.S. law in 2002, many corporate board audit committee–authorizing resolutions were updated to make them compliant. Otherwise, such resolutions are often almost one-time things.

While not a necessary requirement, most corporate internal audit functions regularly operate through a formal internal audit charter, a document (discussed in Chapter 12) that is approved by the audit committee to outline internal audit's role and responsibilities. The Institute of Internal Auditors (IIA) has provided some guidance for drafting an internal audit charter, but such charters do not follow any specific standards or format. They should formally state, among other matters, that internal audit has full access to all records and facilities within the enterprise. Internal audit charters cover the activities of the internal audit function but not the activities of the corporate board audit committee. The NYSE suggested proposed board audit committee charters in December 1999 but with no requirement that an audit committee should have such a charter. SOx, however, has now mandated that each board audit committee must develop its own formal audit charter to be published as part of the annual proxy statement.

The purpose of a board audit committee charter is to define the audit committee's responsibilities regarding:

- Identification, assessment, and management of financial risks and uncertainties
- Continuous improvement of financial systems
- Integrity of financial statements and financial disclosures
- Compliance with legal and regulatory requirements
- Qualifications, independence, and performance of independent outside auditors
- Capabilities, resources, and performance of the internal audit department
- Full and open communication with and among the independent accountants, management, internal auditors, counsel, employees, the audit committee, and the board

The audit committee is required to go before its overall board of directors and obtain authorization, through this charter document, for board audit committee activities just as the CAE, representing the enterprise's internal audit function, regularly goes before the board audit committee.

While some may look on this audit committee charter requirement as additional pages to add bulk to the already thick proxy statement, it is a formal commitment by the board audit committee to ensure the integrity of financial statements and to supervise the internal and external audit functions. There is no single required format or mandated contents for this charter document, but the NYSE has published a model charter that has been adopted by many public corporations today. Formats vary from one enterprise to another, but audit committee charters generally include:

1. Purpose and power of audit committee
2. Audit committee composition
3. Meetings schedule
4. Audit committee procedures
5. Audit committee primary activities
   a. Corporate governance
   b. Public reporting

   c. Independent accountants
   d. Audits and accounting
   e. Other activities
6. Discretionary activities
   a. Independent accountants
   b. Internal audits
   c. Accounting
   d. Controls and systems
   e. Public reporting
   f. Compliance oversight responsibilities
   g. Risk assessments
   h. Financial oversight responsibilities
   i. Employee benefit plans investment fiduciary responsibilities
7. Audit committee limitations

Many audit committee charters contain descriptions of the categories listed. Some appear to have been developed by corporate legal counsels with language to cover every possible contingency while others are more clear and succinct. An excellent example of an easy-to-follow charter is Microsoft Corporation's 2007 audit committee charter, found on its Web site and shown in part in Exhibit 23.2. The full text of that charter also outlines some 30 specific activities for the audit committee. For example, number 29 in that list states: "Meet with the General Auditor in executive sessions to discuss any matters that the Committee or the General Auditor believes should be discussed privately with the Audit Committee" and specifies that this activity will occur two times per year.

Not every corporation is a Microsoft in terms of size and resources, but all corporations with SEC registration must conform to SOx rules. Smaller entities will not have the resources or need to release a Web-based audit committee charter. But they still must have an independent directors' audit committee, as mandated by SOx, as well as an audit committee charter. This is the type of board of directors' resolution document that would be part of corporate records.

Whether larger or small, an enterprise still needs to have effective internal controls and an internal audit function. This is especially important today, as a limited internal audit resource can no longer rely on external auditors to perform tasks they may have performed in the past. The CAE for that smaller corporation should review materials published by the IIA, AICPA, or the Information Systems Audit and Control Association, and work with internal auditors from other smaller firms in the community to develop ideas and approaches. The local IIA chapter typically has member CAEs from nearby similar-size companies who should be willing to share thoughts and ideas. The IIA's Global Audit Information Network program, discussed in Chapter 11, can be a source for reviewing other approaches for developing this material.

23.3 Audit Committee's Financial Expert and Internal Audit

A major audit committee criticism in those pre-SOx days after the fall of Enron was that many board members serving on audit committees did not appear to understand financial and internal control issues. People were elected to board audit committees

EXHIBIT 23.2 Microsoft Corporation 2007 Audit Committee Charter

Role

The Audit Committee of the Board of Directors assists the Board of Directors in fulfilling its responsibility for oversight of the quality and integrity of the accounting, auditing, and reporting practices of the Company, and such other duties as directed by the Board. The Committee's purpose is to oversee the accounting and financial reporting processes of the Company, the audits of the Company's financial statements, the qualifications of the public accounting firm engaged as the Company's independent auditor to prepare or issue an audit report on the financial statements of the Company and internal control over financial reporting, and the performance of the Company's internal audit function and independent auditor. The Committee reviews and assesses the qualitative aspects of financial reporting to shareholders, the Company's processes to manage business and financial risk, and compliance with significant applicable legal, ethical, and regulatory requirements. The Committee is directly responsible for the appointment (subject to shareholder ratification), compensation, retention, and oversight of the independent auditor.

Membership

The membership of the Committee consists of at least three directors, all of whom shall meet the independence requirements established by the Board and applicable laws, regulations, and listing requirements. Each member shall in the judgment of the Board have the ability to read and understand fundamental financial statements and otherwise meet the financial sophistication standard established by the requirements of the NASDAQ Stock Market, LLC. At least one member of the Committee shall in the judgment of the Board be an "audit committee financial expert" as defined by the rules and regulations of the Securities and Exchange Commission. The Board appoints the members of the Committee and the chairperson. The Board may remove any member from the Committee at any time with or without cause.

Generally, no member of the Committee may serve on more than three audit committees of publicly traded companies (including the Audit Committee of the Company) at the same time. For this purpose, service on the audit committees of a parent and its substantially owned subsidiaries counts as service on a single audit committee.

Operations

The Committee meets at least six times a year. Additional meetings may occur as the Committee or its chair deems advisable. The Committee will cause to be kept adequate minutes of its proceedings, and will report on its actions and activities at the next quarterly meeting of the Board. Committee members will be furnished with copies of the minutes of each meeting and any action taken by unanimous consent. The Committee is governed by the same rules regarding meetings (including meetings by conference telephone or similar communications equipment), action without meetings, notice, waiver of notice, and quorum and voting requirements as are applicable to the Board. The Committee is authorized and empowered to adopt its own rules of procedure not inconsistent with (a) any provision of this Charter, (b) any provision of the Bylaws of the Company, or (c) the laws of the state of Washington.

Communications

The independent auditor reports directly to the Committee. The Committee is expected to maintain free and open communication with the independent auditor, the internal auditors, and management. This communication will include periodic private executive sessions with each of these parties.

Source: This charter was taken from Microsoft's SEC-filed 10-K and extracted from its Web site.

(*Continued*)

EXHIBIT 23.2 Microsoft Corporation 2007 Audit Committee Charter (*Continued*)

Education
The Company is responsible for providing new members with appropriate orientation briefings and educational opportunities, and the full Committee with educational resources related to accounting principles and procedures, current accounting topics pertinent to the Company, and other matters as may be requested by the Committee. The Company will assist the Committee in maintaining appropriate financial literacy.

Authority
The Committee will have the resources and authority necessary to discharge its duties and responsibilities. The Committee has sole authority to retain and terminate outside counsel or other experts or consultants, as it deems appropriate, including sole authority to approve the firms' fees and other retention terms. The Company will provide the Committee with appropriate funding, as the Committee determines, for the payment of compensation to the Company's independent auditor, outside counsel, and other advisors as it deems appropriate, and administrative expenses of the Committee that are necessary or appropriate in carrying out its duties. In discharging its oversight role, the Committee is empowered to investigate any matter brought to its attention. The Committee will have access to the Company's books, records, facilities, and personnel. Any communications between the Committee and legal counsel in the course of obtaining legal advice will be considered privileged communications of the Company, and the Committee will take all necessary steps to preserve the privileged nature of those communications.

The Committee may form and delegate authority to subcommittees and may delegate authority to one or more designated members of the Committee.

Responsibilities
The Committee's specific responsibilities in carrying out its oversight role are delineated in the Audit Committee Responsibilities Calendar. The Responsibilities Calendar will be updated annually as necessary to reflect changes in regulatory requirements, authoritative guidance, and evolving oversight practices. The most recently updated Responsibilities Calendar will be considered to be an addendum to this Charter.

The Committee relies on the expertise and knowledge of management, the internal auditors, and the independent auditor in carrying out its oversight responsibilities. Management of the Company is responsible for determining the Company's financial statements are complete, accurate, and in accordance with generally accepted accounting principles and establishing satisfactory internal control over financial reporting. The independent auditor is responsible for auditing the Company's financial statements and the effectiveness of the Company's internal control over financial reporting. It is not the duty of the Committee to plan or conduct audits, to determine that the financial statements are complete and accurate and in accordance with generally accepted accounting principles, to conduct investigations, or to assure compliance with laws and regulations or the Company's standards of business conduct, codes of ethics, internal policies, procedures, and controls.

because of their connections with senior management, business or professional backgrounds but they often did not understand complex financial or internal control issues surrounding many enterprises. SOx now requires that at least one of the audit committee independent directors must be what is called a "financial expert" with some fairly specific requirements for that role, as outlined in the Chapter 4 overview of SOx. This financial expert board member could very well be internal audit's best

or closest audit committee ally and may very well be the starting point for the CAE to closely bind internal audit to the board's audit committee. Today's typical audit committee member and certainly the financial expert are certainly in a new and challenging position with legal mandates and lots of pressure.

SOx has caused many changes to corporate governance, the board of directors, and the audit committee. In many situations, the CAE and internal audit may be a unique thread of corporate governance continuity, and internal audit can help the audit committee in this new era through a three-step approach:

Step 1. Through a report and presentation, provide a detailed summary of current internal audit processes for risk assessments, planning and performing audits, and reporting results through audit reports.

Step 2. Working with human resources and other resources, present plans to the audit committee to assist in launching the Sox-required ethics and whistleblower program as discussed in Chapter 24.

Step 3. Develop detailed plans for reviewing and assessing internal controls in the enterprise. This is a key component of SOx Section 404, internal control assessment requirements, as discussed in Chapter 4.

The first step here is that internal audit should make a concentrated effort to explain its processes and procedures to the audit committee, the overall board, and senior management with an emphasis on SOx's internal audit requirements. Once this board presentation is launched, it should become part of the annual internal audit planning process with ongoing changes reported. However, even before launching any such presentation, internal audit should go through its own processes and perform what might be called a health check to assess current internal audit practices. This check might point to areas where there is ongoing room for internal audit improvement. Exhibit 23.3 is an internal audit health check assessment internal survey that can be expanded or modified depending on current conditions. The idea here is that internal audit should go through a high-level organizational health self-assessment, asking itself how it is doing at present and what it should do to improve, and then making improvements as required. This is also along the lines of a control self-assessment, as discussed in Chapter 11.

Once internal audit has gone through such a self-correction exercise, audit processes and ongoing activities should be presented to the audit committee and the overall board and management. The aim is to make certain that all parties are aware of internal audit's processes and ongoing issues. The information should be presented to key members of management first before the audit committee presentation to ensure that internal audit's message is well understood and consistent with other management initiatives. Depending on the enterprise and its past history, internal audit may receive too little or even too much credit for its role in the corporate governance process.

23.4 Audit Committee Responsibilities for Internal Audit

The board of director's audit committee has a primary responsibility for an enterprise's internal audit function. Prior to SOx, this concept often was little more than theoretical; internal audit reported to the audit committee "on paper" but effectively

EXHIBIT 23.3 Internal Audit Health Check Assessment

Internal Audit (I/A) Processes	Yes / No
1. Does I/A have a formal set of standards and are those standards consistent with IIA Standards (as outlined in Chapter 8)?	
2. Are new I/A members educated on the use of I/A standards, and is overall compliance to standards monitored regularly?	
3. Does I/A prepare an annual audit plan, and is performance against the plan regularly monitored by the audit committee?	
4. Are audit plans developed through a formal risk assessment process (see Chapter 6)?	
5. Are individual audits planned and supervised with sufficient attention given to risks, adequate resources, and staffing (as discussed in Chapter 15)?	
6. Is all I/A work documented through a formal set of workpapers, and are those workpapers reviewed by appropriate levels of management? (Workpaper procedures are discussed in Chapter 16.)	
7. Are audit findings reviewed, as appropriate, with management before release of final audit reports?	
8. Are recipients of audit reports required to respond to recommendations with plans for corrective action and are those responses monitored (see Chapter 17)?	
9. Are there special I/A procedures in place in the event or fraud or suspected fraud encountered during reviews (see Chapter 15)?	
10. Does I/A report the results of its activities regularly to the audit committee?	
11. Are overall budgets developed for all I/A work, and is performance monitored against those budgets?	
12. Do all members of I/A receive adequate training on accounting, internal controls, and technology issues?	

reported to the chief financial officer (CFO) or some other senior corporate officer. The modern internal audit function today should have a charter-defined, very active relationship with the enterprise's audit committee. These charters are often very specific regarding relationships with internal audit and typically require the audit committee to:

- Review the resources, plans, activities, staffing, and organizational structure of internal audit. These areas are discussed in Chapters 12 and 13.
- Review the appointment, performance, and replacement of the CAE.
- Review all audits and reports prepared by internal audit together with management's response. Audit reports and communications are discussed in Chapter 17.
- Review with management, the CAE, and the independent accountants the adequacy of financial reporting and internal control systems. The review should include the scope and results of the internal audit program and the cooperation afforded or limitations, if any, imposed by management on the conduct of the internal audit program.

These points have been part of the relationship between internal audit and its audit committee for some time, but the audit committee charter published in the proxy formalizes this arrangement. The CAE should work closely with the audit

committee to ensure that effective communication links are in place, as discussed in the third bullet point. Some internal audit departments have developed the habit, over time, of supplying their audit committees with just summaries of internal audit report findings or just submitting reports on what internal audit has decided are significant audit report findings. SOx put this in a new perspective. Internal audit should not just send the audit committee what it thinks it needs to see. Rather, SOx mandates that internal audit should provide the audit committee with all audit reports and their supporting management responses. Even when internal audit generates a large number of audit reports, such as for a retail enterprise with audits of many smaller store units that often have few significant findings, the audit committee should receive detailed information on all audits performed. Summary reports can be provided, but complete reports for all audits must be provided as well.

(a) Appointment of the Chief Audit Executive

The CAE typically reports administratively to enterprise management, but the audit committee is responsible for the hiring and dismissal of this internal audit executive. The board's compensation committee may also be involved when the CAE is designated as an officer of the enterprise. The objective here is not to deny enterprise management the right to name the person who will administer the internal audit department, which serves the combined needs of enterprise management and the audit committee. Rather, the significance of the audit committee's participation is to ensure the independence of the internal audit function when there is a need to speak out regarding issues identified in the review and appraisal of internal controls and other enterprise activities.

The actual participation of the audit committee in the selection of the CAE can take a number of forms but typically involves a review of the proposed director's credentials followed by a formal interview. Enterprise management—often primarily the CFO—typically consults with the chair of the audit committee regarding potential CAE candidates, allowing the audit committee time to review and comment, and sometimes interview, before any change is actually made. In many instances, the enterprise will be faced with the need to name a new CAE because the existing person has resigned or has been promoted. Management may suggest the promotion of someone from within the enterprise or may recruit an outsider, but the audit committee will have the final decision. Agreement on the adequacy of the qualifications to serve the needs of both management and the board of directors is an essential condition of an ongoing effective relationship between senior management and the audit committee.

An audit committee usually is not involved in day-to-day administrative matters regarding the CAE and the entire internal audit function but must ensure the ongoing quality of the internal audit function. For example, an incumbent CAE should continue to have opportunities for promotion or be given other responsibilities as a part of a management development program. In other instances, senior management may express strong feelings that the CAE should be transferred or terminated because of some strong management concern. In the latter situation, the audit committee should review the suggested personnel action and provide the CAE with a fair hearing on the issues involved. The audit committee itself may feel that the CAE is not doing an adequate job either in complying with the audit committee's requests or in directing the internal audit function, or both. In such a case, the chair of the

audit committee would typically express those concerns to enterprise management and start the process for a change in personnel. In an extreme case where there is disagreement regarding the CAE, the audit committee can always hire an outside consultant to perform the audit review work desired by the committee or can direct management, through board directives, to make a change.

The overall issue here is that the audit committee has the ability to hire or fire the CAE, but there must be an ongoing level of cooperation. The audit committee generally is not on-site on a daily basis to provide detailed internal audit supervision and must rely on management for some detailed support. The CAE or any member of internal audit cannot just ignore an appropriate management request by claiming he or she reports only to the audit committee and is not responsible to enterprise line management. Similarly, enterprise management must make certain that internal audit is part of the enterprise, not some almost outsider.

(b) Approval of Internal Audit Charter

As discussed in Chapter 12, an internal audit charter serves as a basis or authorization for every effective internal audit program. An adequate charter is particularly important to define the roles and responsibilities of internal audit and its responsibility to serve the audit committee properly. It is here that the mission of internal audit must clearly provide for service to the audit committee as well as to senior management. An internal audit charter is a broad but general document that defines the responsibilities of internal audit within the enterprise, describes the standards followed, and defines the relationship between the audit committee and internal audit. The latter point is particularly important as it sends a special message to senior management that the CAE can go to a higher authority—the audit committee—in the event of a significant controversy or internal controls issue.

The audit committee is responsible for approving this internal audit charter, just as the full board is responsible for approving the audit committee's charter. We are discussing internal audit charters here because of this audit committee responsibility, but internal audit charters were covered in greater detail in the Chapter 12 discussion on charters and building an effective internal audit function. Who is responsible for drafting this internal audit charter? In theory, perhaps, the audit committee might draft this document as a board committee activity. In reality, the CAE will usually take the lead in drafting this charter and/or will suggest appropriate updates to an existing charter to the chair of the audit committee.

While the internal audit charter authorizes the work that should be performed, the audit committee members may not be in a position to draft detailed audit charter requirements. The CAE typically works closely with the chair of the audit committee to draft these requirements. In addition to the charter, the specific nature and scope of internal audit's service responsibilities to the audit committee should be formalized and outlined. These responsibilities could include periodic written audit status reports, regularly scheduled meetings with the audit committee, and both the right and obligation of internal audit's direct access to the audit committee. While this understanding typically does not require a formal audit committee resolution, both parties should have a clear understanding of the responsibilities of internal audit to present reports and to attend audit committee meetings. The acceptance of the internal audit charter and related provisions by all parties of interest means that internal audit is freed from barriers that might otherwise prevent it from

making needed disclosures to the audit committee, even those of a very sensitive nature.

This charter statement of internal audit's relationship to the audit committee is especially important since internal audit also has a day-to-day working relationship with enterprise management. While the audit committee selects the CAE, other members of the audit team are hired and paid by the enterprise, not the independent audit committee. Senior management often forgets that internal audit has this special reporting relationship within the enterprise. Enterprise management sometimes discounts this need for an adequate internal audit charter on the grounds that there are *no restrictions* to internal audit's independence. Nevertheless, a strong internal audit charter, approved by the audit committee, is an important provision of corporate governance.

(c) Approval of Internal Audit Plans and Budgets

Ideally, the audit committee should have developed an overall understanding of the total internal audit needs of the enterprise. This high-level appraisal covers various special control and financial-reporting issues, allowing the audit committee to determine the portion of audit or risk assessment needs to be performed by either internal audit or other providers. As part of this role, the audit committee is responsible for reviewing and approving all internal audit higher-level plans and budgets. This responsibility is consistent with the audit committee's role as the ultimate coordinator of the total audit effort. Enterprise management and the CAE may have their own ideas about what needs to be done, but these actions are an audit committee responsibility. It is essential that the views of the key parties be jointly considered and appropriately reconciled, but the audit committee has the final word here.

The committee's review of all internal audit plans is essential if the policies and plans for the future are to be determined most effectively. New audit responsibilities since the introduction of SOx have changed roles that have been in place for years, and all interested parties should understand the nature of the total audit plan. Enterprise management, internal auditors, and external audit alike then will know what to expect from the suppliers of audit services. The audit committee should assume a high-level coordination role. Although there are practical limitations as to how actively the audit committee can become involved in the detailed planning process, some involvement has a demonstrated high value. Typically, the chair of the audit committee is the most active person in this plan review, but even he or she is subject to time limitations. Internal audit should prepare a comprehensive set of annual planning documents for the committee that give detailed plans for the upcoming year as well as longer-range plans. Suggested formats for these plans are discussed in Chapter 6 on risk analysis and in Chapter 12 on organizing internal audit activities. In addition, internal audit should prepare summarized reports of past audit activities and reassessments of its coverage to give the audit committee an understanding of significant areas covered in past reviews. Although internal audit should report its activities to the audit committee on a regular basis, this summary reporting of past activity gives an overview of areas for audit emphasis and highlights any potential gaps in audit coverage. Exhibit 23.4 is an example of a one-year audit plan for presentation to the audit committee. The CAE would present this type of report to the audit committee, including the particulars for each audit and

EXHIBIT 23.4 One-Year Audit Plan Summary for Audit Committee Review

GLOBAL COMPUTER PRODUCTS 20xx SUMMARIZED AUDIT PLAN

DIVISION	AUDIT	Risk Rank	Est. Start	Planned Finish	Total Hours	Total Costs	Comments
Electro	Inv. Planning Controls	8.4					Carry-over—From 20xx
Electro	Phys. Inv. Observation	9.5					
Electro	B-Plant Security	7.4					
Electro	Materials Receiving	6.2					Physical and Logical Security
Electro	Procurement Controls	6.8					Operational Assessment
Electro	New Marketing System	7.8					
Distribution	XML Order Controls	9.1					First Audit of Process
Distribution	Whse. Physical Security	5.3					Financial Controls
Distribution	Factory Labor Reporting	7.2					Operational Controls
Distribution	Product Incentive System	8.6					Audit Committee Request
Distribution	Prod. Warranty Returns	8.8					Operational Controls
Distribution	Business Continuity Planning	9.1					
Distribution	A/R Control Proceed	7.5					
Asia Pacific	G/L System Integrity	8.6					First Review of Unit
Asia Pacific	Labor Relations Stds.	8.2					First Review of Unit
Asia Pacific	Mfg. Control System	9.2					First Review of Unit
Corporate	Government Relations Dept.	5.3					
Corporate	Construction Contracts	7.3					
Total Internal Audit Projects							
Non-Audit	Training						
Non-Audit	Audit Administration						
Total Internal Audit for 20xx							

with sufficient supporting details to answer questions. The summary report on past activities is particularly important in that it shows the areas scheduled in the prior year's plan and the accomplishments against that plan.

In many enterprises, the annual audit plan is developed through both internal audit's risk analysis process and discussions with both senior management and the audit committee. Management and the committee may suggest areas for potential internal audit review, and internal audit should develop plans within the constraints of budget and resource limitations. If the audit committee has suggested a review of some specialized area but internal audit is unable to perform the planned audit due to some known constraints, the CAE should clearly communicate that deficiency to the audit committee.

(d) Audit Committee Review and Action on Significant Audit Findings

An audit committee's most important responsibility is to review and take action on significant audit findings reported to it by the internal and external auditors, management, and others. While the audit committee has responsibility for all of these areas, our focus here is on the importance of internal audit to report all significant findings to the audit committee regularly and promptly. Part of this reporting will occur through internal audit's distribution of all audit reports to the audit committee as part of the SOx requirements outlined in Chapter 4. While internal audit and others should certainly not filter audit findings and tell the audit committee only what is felt "significant," the interests and efficiencies of all will be better served by internal audit regularly reporting significant audit findings as well as the status and disposition of those findings. Exhibit 23.5 is an example of such a significant findings report from a representative ExampleCo. Corp.

Reacting to significant audit findings requires a combination of understanding, competence, and cooperation by all of the major parties of interest: internal audit, management, external auditors, and the audit committee itself. Total enterprise welfare then becomes the standard by which to judge all internal audit services, as opposed to more provincial views that the interests of management and the audit

EXHIBIT 23.5 Internal Audit Significant Findings Audit Committee Report

Global Computer Products, Inc.
Audit Committee of the Board of Directors
Internal Audit Signficant Audit Findings—May 31, 20XY

Status of Findings Reported in Prior Reports		*Current Status*
JAN XX	San Jose plant continuity plans have not been tested	Open
JUL XX	Physical security at ABC plant space	In process
OCT XX	U.S. Federal Form S-1 Incomplete	Corrected
NOV XX	Poor project planning at Maxx Division	In process
DEC XX	Poor overall plant scrap accounting controls	Corrected
New Significant Audit Report Findings Added		
MAR XY	Poor controls over new WIP system	Open
APR XY	U.S. Federal EEOC reports not filed	Open

committee may be to some extent conflicting. Within its own area of responsibility, internal audit should act aggressively in not just reporting the significant findings but exercising ongoing monitoring actions to assess whether appropriate corrective action items are taken.

23.5 Audit Committee and Its External Auditors

The audit committee has a major responsibility for hiring the external audit firm, approving its proposed budget and audit plan, and releasing the audited financial statements. While many aspects of this arrangement have remained unchanged over time, SOx has caused some significant changes here. As discussed in Chapter 4 on SOx Section 404 internal control assessments, the external auditors no longer can both perform and then approve their internal controls assessments, nor are any consulting arms of public accounting firms allowed to install financial applications that would be subject to external audit review. The major public accounting firms no longer have these consulting divisions, and, as discussed, public accounting firms are prohibited from outsourcing the internal audit services for the enterprises they audit. Audit committees should be aware and sensitive to these changes.

SOx requires that the audit committee approve all external audit services, including comfort letters, as well as any nonaudit services provided by the external auditors. External auditors are still allowed to provide tax services as well as certain *de minimis* service exceptions, but they are prohibited from providing these nonaudit services contemporaneously with their financial statement audits:

- Bookkeeping and other services related to the accounting records or financial statements of the audit client
- Financial information technology design and implementation
- Appraisal or valuation services, fairness opinions, or contribution-in-kind reports
- Internal audit outsourcing services
- Management function or human resource support activities
- Broker or dealer, investment advisor, or investment banking services
- Legal services and other expert services unrelated to the audit
- Any other services that the Public Company Accounting Oversight Board determines to be not permitted

Even though their external auditors are prohibited from performing these activities, corporations still will need to contract for and acquire many of these types of services. These must be treated as special contracting arrangements, reported as part the annual financial reports. It is in the best interests of the external audit firm not to get involved with such nonaudit services. Internal audit should consider offering its services where appropriate and consistent with its charter.

23.6 Whistleblower Programs and Codes of Conduct

As discussed in Chapter 4, SOx rules state the audit committee must establish procedures for the receipt, retention, and treatment of complaints regarding accounting, internal accounting controls, or auditing matters, including procedures for the

confidential, anonymous submission by employees of concerns regarding questionable accounting or auditing matters. This can be a documentation challenge since much of this material must be held in a secure, confidential manner. The CAE as well as the legal counsel often are the only non-CEO and CFO links between the audit committee and the corporation. Internal audit should offer its services to the audit committee—often to the designated financial expert—to establish documentation and communication procedures in these areas:

- **Documentation logging whistleblower calls.** SOx mandates that the audit committee establish a formal whistleblower program where employees can raise their concerns regarding improper audit and controls matters with no fear of retribution. A larger enterprise may already have an ethics function, as discussed in Chapter 24, where these matters can be handled in a secure manner. When a smaller enterprise does not have such a resource, internal audit should offer its facilities to log in such whistleblower communications, recording the date, time, and name of the caller for investigation and disposition. With a heritage of handling secure internal audit reports, internal audit is often the best resource in an enterprise to handle such matters. In all instances, SOx gives the audit committee the responsibility for launching and administering such a whistleblower program.
- **Disposition of whistleblower matters.** Even more important than logging in initial whistleblower calls, documentation must be maintained to record the nature of any follow-up investigations and related dispositions. Although the SOx-mandated whistleblower program does not have any cash reward program, complete documentation covering actions taken as well as any net savings should be maintained. Again, with its tradition of handling confidential matters, internal audit should offer to provide secure, confidential services here. This can be a very important activity. Reporting employees can bring legal action against the corporation if the information they report was leaked and the whistleblowers were retaliated against.
- **Codes of ethics.** SOx makes the audit committee responsible for implementing a code of ethics or conduct for a corporation's senior officers (CEO and CFO). The audit committee must to outline a set of rules for proper conduct and have these senior officers acknowledge that they have read and understand and agree to abide by them. Chapter 24 discusses these ethics and whistleblower programs. Internal audit should play a leading role in helping the audit committee to implement these programs, not just for a limited set of senior officers but for the entire enterprise.

23.7 Other Audit Committee Roles

In this post-SOx world, the audit committee often may receive questions regarding various accounting and auditing matters. Internal audit can offer to act as somewhat of a secretary to the audit committee in documenting and handling these issues. This chapter has outlined many areas where internal audit can help the audit committee in handling some of its new SOx-related administrative chores. Even for a very large corporation, the audit committee may consist of perhaps six persons; in a smaller corporation, the committee typically consists of only two members. In addition, the

typical independent director audit committee member is a busy person who may serve on multiple boards with little direct administrative support. While the CEO's or CFO's administrative support staff usually handles many administrative duties for board members, SOx rules require that the audit committee must act independently. Internal audit can provide the necessary help.

Under SOx, the audit committee takes on an important role, which internal audit is in perhaps one of the best positions to help facilitate. The CAE has open access to the audit committee through presentations at regular meetings and confidential one-on-one meetings. However, in the past, these meetings were often little more than formalities with limited true communications. As discussed throughout this book, SOx has changed these rules.

The audit committee and certainly its designated financial expert now have a whole series of new responsibilities. Internal audit is an excellent source to help audit committee members to fulfill their SOx-related responsibilities through close communications as well as by offering to take on certain audit committee documentation tasks. The broad acceleration of social expectations, their impact on the areas of enterprise responsibility, and the related growth of audit committees have generated new needs for the enterprise. As a result, new and expanding requirements for internal audit services constitute both challenges and opportunities. SOx has changed much here, and the modern internal auditor should be aware of this expanded level of audit committee importance. Internal auditors should both understand these SOx-mandated service needs and actively serve and work with their audit committees as part of an overall objective to provide maximum service to the enterprise.

CHAPTER 24

Ethics and Whistleblower Programs

Internal auditors have always been viewed as the ethical leaders in an enterprise. Whenever there have been questions of questionable dealings or fraud in operations, for example, the management response has always been to call on internal audit to investigate. Because of their strong personal professional standards, supported by well-recognized professional codes of conduct, internal auditors are and should be ethical leaders in the enterprise.

Knowledge and understanding of an internal auditor's professional code of conduct, as discussed in Chapter 8 on internal audit professional standards, is a key internal audit common body of knowledge (CBOK) requirement. Ethics and enterprise-wide codes of conduct have a much larger role in today's enterprise beyond just the internal audit function. For years, many enterprises mouthed words about their commitment to ethics but never went much further. However, starting with a series of major U.S. accounting scandals in the 1980s, the launch of the Committee of Sponsoring Organizations Internal Controls framework in the 1990s, and today's Sarbanes-Oxley (SOx) rules, there has been an almost worldwide emphasis on the importance of establishing an ethical environment throughout the enterprise. While internal audit has had a continuing role here, many of these initiatives also have been launched by other departments, including human resources (HR) and corporate legal. Beyond just promoting an ethical environment for all enterprise stakeholders, enterprise-wide initiatives should emphasize strong individual stakeholder codes of conduct, a recognition of enterprise core values, and whistleblower programs. Today employees and stakeholders at all levels are encouraged to think and act differently from in past years.

Whistleblower programs are an example here. The whole concept behind these programs is that any employee or other stakeholder who observes some work environment matter that is wrong and independently "blow the whistle," or report the matter to senior management, without any fear of recrimination. These concepts have been standard in many U.S. legal rules and have become an element of SOx, as discussed in Chapter 4. While not necessarily the designated recipients of whistleblower reports, internal auditors need to understand the role of whistleblowing and how these activities can fit in the control environment of the enterprise.

This chapter looks at codes of conduct, enterprise ethics, and whistleblower programs from both an enterprise-wide and an internal audit perspective. Internal auditors need to understand these concepts and how they should be applied to the overall enterprise. In addition, in some smaller enterprises with more limited resources, internal audit may be called on to launch and administer many if not all aspects of an enterprise's ethics and whistleblower programs. Knowledge of an internal

auditor's code of conduct is a basic CBOK requirement; an overall understanding of codes of conduct, whistleblower programs, and enterprise ethics is important to the total enterprise and should be a key internal audit knowledge area as well.

This chapter also describes how to establish ethics and whistleblower functions that are consistent with SOx and of value to all enterprise stakeholders: employees, officers, vendors, and contractors. Going beyond the SOx objectives to prevent fraudulent financial reporting, an effective ethics program is an important governance and compliance tool for the entire enterprise. Although whistleblower programs have been a component of U.S. defense contracting labor laws for years, SOx mandates their establishment in all registered public corporations. We look at the guidelines here and things internal audit can do to establish effective programs in the enterprise. This chapter also briefly looks at the Organizational Sentencing Guidelines, a U.S.-based carrot-and-stick judicial approach to promote strong enterprise compliance programs. The chapter concludes with guidelines for performing operational and compliance audits over these functions.

24.1 Enterprise Ethics, Compliance, and Governance

Investigators, regulators, and journalists have stated that many of the high-profile business failures over recent years, in the United States and elsewhere, occurred because of unethical behavior by business managers at all levels. Historically, such failures are nothing new. Ethical lapses have occurred since the early days of business and trade—at least over the past 1,000 years. However, today's lapses often seem different: The media publicizes the information widely, and many more people may be hurt due to their stock market investments, retirement accounts, and other financial interests. The attitude of the so-called robber barons of the 1880s—"Let the public be damned!"—is not acceptable in today's society, when there is increased interest in business ethics, codes of conduct, and enterprise governance issues.

Internal auditors have been familiar with ethics programs and codes of conduct for years. A code of conduct is a prominent component of internal audit's professional standards, and many internal auditors have become involved with reviewing and helping to enhance their enterprise's ethics programs. This area became even more important when SOx mandated signed ethics or code of conduct statements from senior officers and called for whistleblower programs directed by the audit committee.

As outlined in Chapter 4, SOx mandates that corporate audit committees must have their chief financial officer (CFO) sign an ethics statement. While this is no guarantee that the CFO will always follow ethical business practices, the personal risks of a major fine or even prison are strong inducements. However, a strong set of personal values throughout the enterprise as well as an ongoing commitment or desire to always do the right thing are often even more important. While SOx's requirements are limited to senior financial officers, an enterprise will generally find more value in launching and implementing such a program for the entire enterprise and its key stakeholders. Some ethics and code of conduct rules are very specific and pertain just to the financial officers; however, enterprises will find greater value in having one set of rules apply to all, and internal audit may want to consider advising management to move in that direction.

Enterprises of all sizes and areas of business today should establish effective ethics functions, including a mission statement and a code of conduct. Although an enterprise ethics program is important today, an enterprise cannot claim to have implemented such a program by just publishing an organizational code of business conduct along with instructions for all employees to read it. An effective ethics program requires a formal commitment between the enterprise and its employees and agents to do the right thing. Many enterprises today already have elements of an ethics program in place; others assume they have good ethics practices because there have been no recent problems. All too often, those established "ethics programs" amount to little more than an employee code of conduct given to new hires on their first day on the job plus perhaps a few employee posters or brochures. New employees are asked to read and sign the enterprise's code of conduct as part of completing such new hire materials as tax withholding forms, medical plan selections, and other employee options. All too often the code of conduct is signed, filed away, and forgotten. This does not constitute an effective ethics program for an enterprise.

An effective ethics program for an enterprise starts with understanding the risk environment and then requires an effective code of conduct. While the emphasis may be a bit different at various levels, everyone should be aware of the enterprise's values and overall mission. As a natural party interested in good, ethical business practices, internal audit should be in a key position to help launch an enterprise-wide ethics function if one does not exist or to help to improve any current programs. Just as internal auditors should understand how to evaluate and recommend effective internal accounting controls, they should have a basic understanding of the elements of an effective organization ethics program.

(a) Ethics First Steps: Developing a Mission Statement

Every enterprise, no matter what size, should have a formal mission statement to describe its overall objectives and values. Properly developed, a mission statement should be a source of direction—a compass—to let employees, customers, stockholders, and other stakeholders know what the enterprise stands for and what it does not. Once little more than tired-sounding slogans, effective enterprise mission statements have become very important for promoting strong organizational ethics and good corporate governance. Effective mission statements can be a great asset to an, enterprise allowing it to better achieve organizational goals and purposes.

The Johnson & Johnson Tylenol® crisis of the early 1990s provides a good example of the importance of a strong corporate mission statement as a compass. Johnson & Johnson, a major medical products provider, manufactured a popular pain reliever medication called Tylenol. In those days, such medications were sold in stores over the counter in screw-top bottles. Someone in the Chicago area opened a number of these Tylenol bottles, adulterated their contents with cyanide poison, and placed the bottles back on the store shelves. Several people who purchased this tainted Tylenol subsequently died. An investigation of these deaths quickly pointed to Johnson & Johnson and the poison-tainted Tylenol.

This whole matter put Johnson & Johnson under massive pressure. The corporation knew that it had extremely strong quality control processes in place that would prevent such poison contamination within its own manufacturing facilities. It also knew that the contaminated products had appeared only in the Chicago area,

even though Tylenol was found on store shelves worldwide. A total product recall would be extremely expensive. However, rather than going through a lengthy series of internal investigations, Johnson & Johnson quickly did the right thing. It recalled all Tylenol from store shelves worldwide and subsequently rereleased it in a newly designed sealed package. When asked why it was able to make such a very expensive recall decision so quickly even though the company knew it was not at fault, the corporation stated that there was no need for a delayed decision. The Johnson & Johnson Credo, its mission statement, dictated the decision. That credo, found on the Johnson & Johnson Web site (www.jnj.com/our_company/our_credo/index.htm) states very strongly that the company's first responsibility is to supply high-quality products to customers. At the time of the Tylenol crisis, everyone at Johnson & Johnson knew this, the credo had been posted widely in enterprise facilities, and there was no need for a decision. The whole unfortunate matter highlighted the importance of a strong mission statement for an enterprise.

A strong corporate mission statement is an important element in any ethics and corporate governance initiative. Although most enterprises will not face a crisis like what Johnson & Johnson did with tainted Tylenol, a stronger anchor of this sort might have helped some enterprises to better avoid the accounting scandals that led to SOx.

Working with an ethics officer function and senior management, internal audit can help to evaluate mission statements or rewrite and launch new ones. Stakeholder ethics surveys discussed in the next section highlight potential problems in mission statements. If employees or other stakeholders are not aware of the corporate mission statement or if they view it as little more than a set of meaningless words, there is a need to revisit and revise that document. A poorly crafted mission statement often does more harm than good, creating cynical and unhappy organizational members who resist change. If the enterprise has no mission or values statement, internal audit should recommend assembling a team to develop a statement that reflects the enterprise's overall values and purposes. If an existing statement was met with cynicism during the ethics survey, it is time to rework and revise it. However, any revised statement should be carefully crafted and delivered. If just rolled out with no preparation, it may be viewed with even more cynicism. A good mission statement also is a good starting point for the senior management tone-at-the-top messages.

A good mission statement should make a positive statement about an enterprise and inspire enterprise stakeholders to harness their energy, passion, and commitment to achieving goals and objectives. The idea is to create a sense of purpose and direction that will be shared throughout the enterprise. Perhaps one of the best examples of a mission statement was expressed by U.S. President John F. Kennedy in the early 1960s:

> *This nation should dedicate itself to achieving the goal, before this decade is out, of landing a man on the moon and returning him safely to Earth.*

Those simple words describe a mission and vision much better than an extensive document of many pages. Sometimes called values statements or credos, this type of statement is often printed in annual reports. Some are lengthy with detailed content; others seem to be little more than fluff. The best are closer to the Johnson & Johnson Credo or Kennedy's moon landing statement in style.

Once an enterprise has developed a new mission statement or has revised an existing one, it should be rolled out to all enterprise members with a good level of publicity. Using a tone-at-the-top approach, senior managers should explain the reasons for the new mission statement and why it will be important for the enterprise. It should be posted on facility billboards, in the annual report, and elsewhere to encourage all stakeholders to read and accept it. The mission statement, however, should just not stand by itself. A series of other key steps are needed to build an effective ethics and compliance function.

Sometimes an internal auditor might argue: "I'm an internal auditor—I just review the controls that are in place. What do I have to do with launching an ethics function?" Internal audit should always be involved with reviewing and commenting on the controls that others have established. However, due to the unique nature of ethics and compliance programs and their relationship to the overall enterprise, internal audit can take an even more active role in helping to implement them.

(b) Understanding the Ethics Risk Environment

Virtually every enterprise faces a mix of risks that limit its business operations, growth, profitability, or other areas. In the aftermath of the dot-com bubble of the 1990s,[1] many businesses faced the risk of severe downturns. In order to keep growing and show ever-increasing growth as the dot-com era was beginning to slow down, too many enterprises bent rules regarding their financial performance. This was the path of Enron, WorldCom, and others, and also led the U.S. Congress to pass SOx. Understanding an enterprise's risk environment is a first step to launching an effective ethics program.

An effective ethics program cannot shield an enterprise from the risk of a major earthquake or some other cataclysmic event; it can, however, help to shield it from a variety of other operational and business risks. Just as some accounting officers decided to bend the rules prior to SOx, attitudes that it is acceptable to ignore ethics rules can present risks in many other areas. The office worker who copies company software or records it for use on the home computer, the factory worker who skips product final inspection procedures to save time, or the vendor that ships fewer items than ordered because "they never check" shipping notices are all examples of bending rules and increasing risks to the enterprise. These kinds of practices often develop because of perceived disparities between senior management and staff. The employee who regularly sees managers exceed expense account limits with no repercussions may soon try to bend the rules in other areas.

Internal audit can take a major lead here in surveying employee attitudes and practices. Ethics attitudes and risks can be assessed through either targeted reviews of findings from past audits or special reviews based on employee and stakeholder ethics attitude surveys. Internal audit can accomplish this ethics survey work through coordination with the enterprise's ethics function, if such a group exists. The nature of such an ethics functions is discussed in the paragraphs to come. If a formal ethics function exists, internal audit should review the results of any surveys that performed there, making plans to revise or update as necessary. An ethics survey is a very good way to understand enterprise attitudes and is an aid to support corporate governance processes.

(i) ETHICS-RELATED FINDINGS FROM PAST AUDITS OR SPECIAL AUDITS If internal audit has completed a large number of compliance-related operational and financial audits recently, a reexamination of workpaper and audit report findings or even responses may provide insight into overall ethical attitudes. Consistent workpaper findings covering "minor" infractions may point to overall trends in ethical attitudes. An example here would be an ongoing failure of employees to follow some relatively minor process or procedures, such as securing a second approval signature on smaller-valued transactions, despite a policy calling for this second signature, or the failure to document new information technology applications, despite systems development documentation requirements. The responsible audit team may have decided the matter was "too minor" to include in summarized final audit reports, but such findings often point to potential ethical attitude problems. Even worse, sometimes these types of findings are reported in audit reports only to be brushed off in the report responses.

Some of the ongoing "minor" findings mentioned may not point to ongoing ethical violations but to areas where rules just need to be changed. Some enterprises, for example, may have travel expense rules calling for *every* travel expense to be supported with a receipt, even if this includes highway tollbooth fares of 50 cents. The driver can get this toll receipt only by waiting in the cashier line rather than driving through a faster line that accepts coins without receipts. Because managers and others may feel that rules requiring such small-value receipts do not add value, expense reports lacking these receipts may be submitted and approved without these receipts. Such a matter may be noted but certainly not reported in audit reports. From an internal audit perspective, does this situation represent an ethical violation for the enterprise? On one level, the answer may be yes, because a rule is a rule. However, an internal auditor reviewing past audit reports and workpapers for ethical problems might best work with the appropriate unit in the enterprise to get such unreasonable rule procedures changed. Internal audit might also consider launching a special audit to assess such ethical attitudes. This would be a strong compliance review covering some key areas across the enterprise or a highly focused review in one department or group. This type of internal audit–review provides an overall assessment of ethical attitudes in the enterprise.

(ii) EMPLOYEE AND STAKEHOLDER ETHICS ATTITUDE SURVEYS Properly done, employee, officer, and stakeholder surveys can be an excellent way to assess enterprise ethical attitudes. The idea is to gather as much information as possible about ethical attitudes and practices from broad groups in the enterprise, such as factory workers (if appropriate), office staff, senior managers, vendors, and others. The survey would include some common questions, but each group would also receive specific questions directed to its responsibilities. The senior officer group, for example, would receive the same set of organizational attitude questions given to all but get specific SOx internal control–related questions.

It is never easy to draft a fact-gathering survey that receives a high response level, and the use specialized help should be considered. Rather than a series of questions requiring just yes-or-no responses, the survey should consist of many "Have you ever. . ." questions where persons completing the survey can provide as long or as short an answer as they wish. Open-ended responses makes compiling the results more difficult, but interesting and valuable information may be gained.

EXHIBIT 24.1 Ethics Environment Attitude Survey Questions

These questions might be used by an internal auditor in a survey of managers, supervisors, and other enterprise professionals in order to gain an better understanding the ethics environment.

1. Do you have access to current enterprise policies and procedures?
2. If you have questions or need clarifications regarding these procedures, do you have a mechanism to ask questions or seek advice?
3. When an established procedure does not appear applicable, given current conditions, is there a process for submitting it for review?
4. Do you feel the rules and procedures apply just to other groups, such as regular employees if you are part time or the headquarters operation if you are at a remote subsidiary?
5. Do you feel your senior managers follow the same types and levels of rules that you follow?
6. Has your supervisor ever told you to ignore some rule or procedure?
7. Do you feel some of the published rules and procedures are trivial or out of date?
8. Do you feel the chief executive officer and other senior officers have delivered clear and strong messages on the importance of enterprise ethics?
9. Are you familiar with the enterprise's mission statement?
10. What does the mission statement mean to you?
11. Are you familiar with code of business conduct?
12. Do you feel this code of conduct is regularly updated to reflect current business activities and issues?
13. Do you feel the code of conduct is applicable to all stakeholders, such as officers, contractors, and vendors?
14. Do you feel the rules are clear for violations of the code of conduct?
15. Have you ever reported an observed code of conduct violation? Were you satisfied with the results of that reporting?
16. Have you ever participated in any enterprise-sponsored ethics training?
17. Do you feel that training was relevant to your work environment as well as your duties and responsibilities?
18. Do you understand how to report accounting, internal control, or auditing concerns under the enterprise's whistleblower program?
19. Do you feel there is an effective mechanism in place to confidentially report violations of the code or other questionable acts?
20. Do you feel there are effective processes in place to investigate reported compliance violations and then to resolve them?
21. Have you observed any evidence that reported ethics compliance violations are subject to disciplinary action?
22. Would you be reluctant to report a violation for fear of potential employer retaliatory actions?

Exhibit 24.1 is an example of an ethics attitude survey that might be directed to supervisory, management, and other professional members of the enterprise.

A key requirement of this type of survey is that it must be as anonymous as possible. The surveys should be sent directly to employee homes along with a cover letter from the chief executive officer (CEO) explaining their objectives and purpose. Return envelopes, prestamped, directed to a special post office box should be included. The primary objective here would be to survey ethics attitudes; however, if the enterprise has already established a whistleblower hotline function, as will be discussed,

the survey could also allow people to report such matters. Summarizing survey results can be a major challenge, particularly if respondents have provided free-form responses. Internal audit or the ethics officer would be responsible for preparing the summary report with an objective of reviewing results with the audit committee and senior managements. For confidentiality reasons, respondents would not receive this summary report; they should receive only a general thank-you type of letter.

Ethics surveys will allow internal audit, a designated ethics office team, or others to gain a general understanding about the ethics environment in the enterprise. This can be a first step to launching a formal ethics function or upgrading and enhancing an existing one. These surveys also will provide general management with some insight into the overall ethics atmosphere in the enterprise. While not required under SOx, this information will bolster corporate governance practices by highlighting areas where improvements are needed.

(c) Summarizing Ethics Survey Results: Do We Have a Problem?

The results of an ethics attitude survey or assessments from past internal audits may provide some assurances that things are pretty good throughout the enterprise. More often, however, they can raise some troubling signs ranging from small but ongoing compliance deviations, to surveyed vendors claiming heavy-handed negotiation tactics, to employees stating they have been asked to bend rules. The hard question with any such results is whether they represent troubling exceptions or the tip of a much larger ethics problem iceberg. At this point, internal audit and the enterprise's ethics officer should meet with senior management to develop some next steps.

Based on any potential disturbing red flags from the surveys, it may be best to expand the mail survey process. Also, concerns that came out of those initial surveys may point to a need to expand the assessments to such groups as customers, agents, or vendors. If the survey results ended with inconclusive or mixed messages, another appropriate step would be to set up a series of focus group sessions. Small groups of employees and stakeholders would be randomly selected and asked to meet in an off-site location to discuss their perceptions of organizational ethical values. A skilled facilitator who emphasizes that any responses from such sessions are anonymous, could lead the group through a discussion. The resultant data may form the basis for launching an enterprise-wide ethics program or enhancing any existing programs. As will be discussed, an ethics program effort also requires a strong code of conduct as well as a whistleblower process to allow for reporting of ethics violations.

As mentioned, SOx talks about these ethics and whistleblower issues only in terms of senior financial officers and potential financial fraud. A strong, effective ethics program, however, will benefit the entire enterprise in addition to providing SOx compliance. If the enterprise does not already have an established ethics program, internal audit is a logical area to help establish this type of program.

24.2 Enterprise Codes of Conduct

While a mission statement is a keystone to hold together the overall structure of corporate governance, an enterprise code of conduct provides the supporting guidance for its stakeholders. SOx uses the phrase *code of ethics*; we are using the more traditional name *code of conduct*. These codes have been in place at major corporations for many years. SOx requires that all registrants develop such a code for

senior financial officers to promote the honest and ethical handling of any conflicts of interest and compliance with applicable governmental rules and regulations. Even if an enterprise does not come under SOx rules, there are many benefits to developing and issuing an appropriate code of conduct. The SOx code is mandated, but enterprises of any size can benefit from a code that covers all stakeholders.

The effective enterprise today should develop and enforce a code of conduct that covers applicable ethical, business, and legal rules for all enterprise stakeholders: the financial officers highlighted in SOx, all other employees, and a larger group of stakeholders. Internal audit is not typically the catalyst group to draft or launch such a code of conduct, but it can be a key participant in both helping to launch the code and then determining that the code promotes ethical business practices throughout the enterprise.

(a) Code of Conduct Contents: What Should Be the Code's Message?

A code of conduct should be a clear, unambiguous set of rules that outlines what is expected of all enterprise stakeholders, officers, employees, contractors, vendors, and others. The code should be based on both the values and legal issues surrounding an enterprise. That is, while all enterprises can expect to have code of conduct prohibitions against sexual and racial discrimination, a defense contractor with many contract-related issues might have a somewhat different code of conduct from a fast food store operation. However, the code should apply to all members of the enterprise from the most senior level to a part-time clerical employee. For example, a code of conduct rule prohibiting erroneous financial reporting is the same whether directed at the CFO for incorrect quarterly financial reporting or the part-timer for an incorrect or fraudulent weekly time card.

If the enterprise already has a code of conduct, internal audit may want to schedule a review from time to time to revisit that code. All too often, older codes were originally drafted as rules for lower-level employees with little attention for the more senior members of the enterprise. As we have discussed, SOx overall corporate governance guidance was meant for senior officers, but it should also apply to all enterprise stakeholders. Working with senior members of management and the audit committee, internal audit can examine any existing code of conduct to determine if those rules still fit for the post-SOx era.

A joint team from a cross-section of management, including legal and human resources, should be assembled to develop or revise the code. The team should examine the business issues facing the enterprise and draft a set of rules applicable to it. The rules must be written in a clear manner such that the points can be easily understood by all. Exhibit 24.2 lists some example code of conduct topics. This list, although it does not apply to all enterprises, includes topics that are appropriate for many modern enterprises. The key is that messages delivered in the code must be clear and unambiguous.

Some years ago this author led a project to develop and implement a code of conduct for a large U.S. corporation. An extract from the code's section on company assets reads:

> *We all have a responsibility to care for all of the company's assets including inventory, cash, supplies, facilities, and the services of other employees and computer systems resources. If you see or suspect that another employee is stealing, engaging in fraudulent activities, or otherwise not properly protecting company assets, you may report these activities to your manager or to the ethics office.*

EXHIBIT 24.2 Code of Conduct Topics Example

These topic areas are found in a typical enterprise stakeholder code of conduct. The actual code should have specific rules in each of these areas.

I. Introduction
   - **A.** Purpose of this code of conduct: A general statement about the background of the code of conduct, emphasizing enterprise traditions.
   - **B.** Enterprise's commitment to strong ethical standards: A restatement of the mission statement and a supporting message from the chief executive officer.
   - **C.** Where to seek guidance: A description of the ethics hotline process.
   - **D.** Reporting noncompliance: Guidance for whistleblowers—how to report.
   - **E.** Your responsibility to acknowledge the code: A description of the code acknowledgment process for all stakeholders.

II. Fair Dealing Standards
   - **A.** Enterprise selling practices: Guidance for dealing with customers.
   - **B.** Enterprise buying practices: Guidance and policies for dealing with vendors.

III. Conduct in the Workplace
   - **A.** Equal Employment Opportunity Standards: A strong commitment statement.
   - **B.** Workplace and sexual harassment policies: An equally strong commitment statement.
   - **C.** Alcohol and substance abuse: A policy statement in this area.

IV. Conflicts of Interest
   - **A.** Outside Employment: Limitations on accepting employment from competitors,
   - **B.** Personal investments: Rules regarding using enterprise data to make personal investment decisions.
   - **C.** Gifts and other benefits: Rules regarding receiving bribes and improper gifts.
   - **D.** Former employees: Rules prohibiting giving favors to ex-employees in business.
   - **E.** Family members: Rules about giving business to family members, creating potential conflicts of interest, and family member employee relationships.

V. Enterprise Property and Records
   - **A.** Enterprise assets: A strong statement on the employees' responsibility to protect assets.
   - **B.** Computer systems resources: An expansion of the enterprise assets statement to reflect all aspects of computer systems resources.
   - **C.** Use of the enterprise's name: A rule that the enterprise name should be used only for normal business dealings.
   - **D.** Enterprise records: A rule regarding employee responsibility for records integrity.
   - **E.** Confidential information: Rules on the importance of keeping all enterprise information confidential and not disclosing it to outsiders.
   - **F.** Employee privacy: A strong statement on the importance of keeping employee personal information confidential to outsiders and even other employees.
   - **G.** Enterprise benefits: Employees must not take enterprise benefits to which they are not entitled.

VI. Complying with the Law
   - **A.** Inside information and insider trading: A strong rule prohibiting insider trading or otherwise benefiting from inside information.
   - **B.** Political contributions and activities: A strong statement on political activity rules.
   - **C.** Bribery and kickbacks: A firm rule of using bribes or accepting kickbacks.
   - **D.** Foreign business dealings: Rules regarding dealing with foreign agents in line with the Foreign Corrupt Practices Act.
   - **E.** Workplace safety: A statement on the enterprise policy to comply with OSHA rules.
   - **F.** Product safety: A statement on the enterprise commitment to product safety.
   - **G.** Environmental protection: A rule regarding the enterprise's commitment to comply with applicable environmental laws.

These words are an example of the tone and style of a good code of conduct. It places the responsibility on the recipient of the code, tries to explain the issues in an unambiguous manner, and suggests expected responses and actions.

Many enterprises have found value in adding a set of frequently asked questions (FAQs) to the code along with suggested answers. FAQs allow readers to better understand issues, questions, and rules. The team drafting a new or revised code of conduct must ensure that it is clear and understood by all. This can be a real editing challenge.

Codes of conduct for different enterprises look different in terms of style, format, and size. Some codes are elaborate documents; others are very bare bones. Enterprise codes of conduct are readily available through corporate Web sites or ethics or internal audit departments. It is suggested that teams revising a corporate code contact enterprises in their industry to examine their codes.

Global enterprises face another issue when developing a code of conduct. Although a corporation may be headquartered in the United States, it may have significant operations worldwide, where key managers, employees, and other stakeholders do not use English as their prime language. Despite the added costs of translation, firms should consider producing a version of the code in at least the major languages used in corporate operations. If there are many locations and just small numbers of various foreign-language stakeholders, a summary of the main code of conduct in each of the local languages might be appropriate. However, those summary versions should certainly emphasize the same SOx financial fraud guidance contained in the prime code of conduct.

(b) Communications to Stakeholders and Assuring Compliance

An enterprise's code of conduct must be a *living document*. It has little value if it has been developed, delivered to all stakeholders with much hullabaloo, and then essentially filed and forgotten. If the document represents a new code of conduct or even a major revision, the enterprise should undertake a major effort to deliver a copy conduct to all employees and stakeholders. Given our current SOx rules, a good first step would be to formally present the new code to the enterprise's top managers, particularly the financial officers. In the past, codes of conduct sometimes received only token acceptance from the senior officer group, who felt the documents were really for the staff, not them. The financial scandals that led up to SOx highlighted this discrepancy. Both Enron and WorldCom had adequate corporate codes of conduct, but their corporate officers evidently did not feel these rules applied to them.

The senior management group should then formally acknowledge that they have read, understand, and will abide by the code of conduct. With the management team standing behind the code, the enterprise should next roll out and deliver the code to all enterprise stakeholders. This can be done in multiple phases with delivery to local or more major facilities first followed by smaller units, foreign locations, and other stakeholders. Rather than just including a copy of the code with payroll documents, an enterprise should make a formal effort to present the code in a manner that will gain attention.

A new code of conduct can be communicated through a video by the CEO, Webcasts, training sessions, or other means to emphasize its importance. Special communication methods might be used for other groups, such as vendors or contractors, but an enterprise should aim to get all stakeholders to formally acknowledge

that they will abide by the code of conduct. This can be accomplished by an Internet or telephone response system, where every enterprise stakeholder is asked to respond to three questions:

1. Have you received and read a copy of the code of conduct? Answer Yes or No.
2. Do you understand the contents of the code of conduct? Answer Yes if you understand this code of conduct or No if you have questions.
3. Do you agree to abide by the policies and guidelines in this code of conduct? Answer Yes if you agree to abide by the code and No if you do not.

Responses should be recorded on a database listing the employee name and the date of their review and acceptance or nonacceptance. Any questions from item 2 can be handled through the whistleblower program described in Section 24.3. If someone refuses to accept the code because of questions, supervisors or others should discuss the matter with that person to gain eventual resolution. The enterprise should expect all employees to agree to accept and abide by its code of conduct. Following that code of conduct is just another work rule, and consistent failure to abide by these rules should be grounds for termination.

This code acknowledgment requirement prevents employees from saying "I didn't know that was the rule" when they violate or see someone violate the code. It is a good idea to go through code acceptance process annually or at least after any revisions. The files documenting these code acknowledgments should be retained in a secure manner.

(c) Code Violations and Corrective Actions

An enterprise-wide code of conduct lays out a set of rules for expected behavior in the enterprise. In addition to publishing a code of conduct and obtaining stakeholder acceptance, there also is a need for a mechanism to report code violations and for investigating and handling those violations.

If the enterprise issues a strong code of conduct along with a message from the CEO about the importance of good ethical practices, all stakeholders are expected to follow those rules. However, people are people, and there will always be some who violate the rules or run on the edge. An enterprise needs to establish a way to allow employees or outsiders to report potential violations of the code in a secure manner and confidential manner. Much of that reporting mechanism can be handled through the whistleblower facility, as discussed in Section 24.3. Other potential violations must be handled on a different level. Consider the female staff employee with a male supervisor who "hints" that sexual favors with him are a good way to advance in the enterprise. A sexual harassment prohibition in the code of conduct will not necessarily stop the supervisor, and often employees cannot easily report the situation to a manager one level above the supervisor.

In addition to the whistleblower facility, the enterprise should establish other mechanisms for reporting potential code of conduct violations. Since some people may not want to call an ethics hotline function, a well-publicized post office box address is sometimes very effective. Stakeholders could be encouraged to mail a letter to such a PO box, anonymously or not, to report ethics violations. Based on these responses, the ethics function, Human Resources (HR), or some other appropriate function in the enterprise should investigate the matter and take action as necessary.

A code of conduct describes a series of rules for expected actions in the enterprise. When these rules are violated, the matter should be investigated and actions taken on a consistent basis, no matter what rank the enterprise stakeholders. If the code of conduct prohibits making copies of corporate software—and it should—the penalties for a staff analyst in a remote sale office or a senior manager in corporate headquarters should be the same. Assuming they both read the prohibition in the code and acknowledged acceptance, penalties for violations should be consistent. Otherwise, the rules will appear to apply only to some.

Most code of conduct violations can be handled through the enterprise's normal HR procedures, which should have established processes where a first offense might result in verbal counseling or probation with termination for repeated violations. Some matters must be reported to outside authorities. A violation of SOx rules, such as a recently discovered undocumented off-balance sheet arrangement, would be reported to the Securities and Exchange Commission (SEC); theft of goods from a warehouse would be reported to a county prosecutor. When these matters are discovered and reported to outside authorities, the matter moves outside the enterprise's control. The overall goal here is for the enterprise to have some process in place to encourage all stakeholders to follow good ethical practices, as defined in the code of conduct, and to provide a consistent mechanism for reporting violations and taking disciplinary action when necessary.

(d) Keeping the Code of Conduct Current

Many of the basic rules of good ethical behavior and many enterprise-specific rules will not change from year to year. For example, the rule that states that all stakeholders have a responsibility to care for their enterprise's assets, whether property, cash, computer resources, or others, rule will not change over time. Enterprises should review their published codes of conduct periodically, at least once every two years, to make certain the guidance is still applicable and current. This periodic review might include a code statement regarding the need for accurate and timely financial reporting at all levels or the enterprise's commitment to avoid any type of financial fraud. Changes to the code of conduct should not be treated lightly. Any revision should go through the same announcement and rollout process as described for code introductions. The revised code should be issued to all stakeholders along with an explanation of the changes and a requirement to reacknowledge acceptance.

As new employees and other stakeholders join an enterprise, they should be given the existing code of conduct with the same requirement that they read and affirm the document. Consideration might be given to an online video to explain and educate new employees regarding the code of conduct and the enterprise's commitment to it. Also, whether the code is revised or not, all stakeholders should be asked periodically to reaffirm that they have read and will continue to abide by the code.

A code of conduct revision and request for stakeholder reaffirmation can be expensive, requiring dedicated enterprise resources from the ethics function, HR, internal audit, and others. Along with the mission statement, an enterprise should keep its code of conduct and supporting principles in front of all stakeholders at all times. This can be accomplished through constant references to the code, such as in bulletin board posters in all facilities, instructive questions and answers in publications, or segments in employee training classes. Internal audit should play a

key role in promoting the code and monitoring compliance through audit reviews and ongoing contacts throughout the enterprise. Internal auditors should be very aware of their enterprise's code of conduct and use it as a basis for reporting violations and making recommendations during all other internal audits.

24.3 Whistleblower and Hotline Functions

During the tumultuous periods prior to the failures of Enron and WorldCom, employees at each of those companies saw some of the severe accounting problems that eventually caused their companies' failures. Several employees did not feel they could communicate these concerns to their immediate supervisors and instead reported to senior management. Even though those reports were all but ignored, whistleblower protections have been part of many federal labor laws as a means to help regulators ferret out violations and wrongdoing. As outlined in Chapter 4, SOx mandates that enterprise audit committees establish procedures to "handle whistleblower information regarding questionable accounting or auditing matters." The whistleblower provisions of SOx are patterned after similar statutory schemes for protecting workers in the airline and nuclear power industries.

A whistleblower function is a facility where an employee or stakeholder who sees some form of wrongdoing can independently and anonymously report that action to the enterprise or to regulatory authorities with no fear of retribution. Whistleblower programs have been around for some years to support U.S. federal contracting laws, health and safety regulations, and others. SOx, however, has moved these rules into the business offices of all U.S. publicly traded enterprises. The audit committee establishes these whistleblower procedures, but other functions, such as the ethics department, HR, or internal audit, actually set them up.

Many enterprises that have established ethics functions also have a hotline or similar ethics question telephone lines. These ethics hotlines can provide a starting point for the SOx whistleblower function, but they typically need adjustments or fine-tuning. Too often, reported incidents are not investigated properly or confidentiality is not as strong as necessary. A slip-up here can cause major problems for an enterprise if the whistleblowing stakeholder feels matters have not been resolved or individual confidentiality has been compromised. Internal audit often can be a major aid here through reviews of the existing process, recommending appropriate controls, and providing guidance to the audit committee.

Following the U.S. whistleblower rules for federal contracting and other federal regulations, any employee or stakeholder who observes some type of improper activity can blow the whistle and report the incident. The matter is then to be investigated and corrected if the allegations prove true. For example, say an employee observes that a manufactured food ingredient appears to be lacking proper safety inspections. He or she can inform the employer about this potential violation.

SOx-mandated whistleblower programs present audit committee members with another challenge. The typical board of directors' audit committee member *may* be aware of such an enterprise function through past presentations but almost certainly will not be aware of the necessary processes to establish an effective whistleblower program. Internal audit groups can help the audit committee representative to establish an effective whistleblower program that will comply with SOx. This section

discusses how to establish effective whistleblower programs and how internal audit can help to launch or refresh the function.

(a) Federal Whistleblower Rules

The U.S. Department of Labor (DOL) administers and enforces more than 180 federal laws covering many workplace activities for about 10 million employers and 125 million workers. Most labor and public safety laws and many environmental laws mandate whistleblower protections for employees who complain about violations of the law by their employers. SOx has expanded this federal whistleblower protection. SOx Section 806 establishes whistleblower protection for stakeholders in publicly traded companies, stating that no public company or any officer, employee, contractor, or agent of such company "may discharge, demote, suspend, threaten, harass, or in any other manner discriminate against an employee in the terms and conditions of employment because of any lawful act done by the employee." Those "lawful acts" are when the employee provides information or otherwise assists in an investigation conducted by a federal regulatory or law enforcement agency, Congress, or company personnel regarding any conduct that the employee "reasonably believes" constitutes a violation of SEC rules and regulations or fraud statutes; or files, testifies, participates in, or otherwise assists in a proceeding—pending or about to be filed—relating to an alleged violation. In other words, the employee or stakeholder who perceives some financial wrongdoing and then reports the matter is legally protected as part of the whistleblower investigation and resolution.

In many respects, whistleblower provisions are designed primarily to protect employees who think they have discovered some wrongdoing rather than to increase enterprise internal controls. Virtually any personnel action taken against a whistleblower employee, including a demotion or suspension, can potentially be subject to legal action under this provision. Although there have not been many whistleblower matters related to SOx at present, if the experiences from other whistleblower statutes are applied here, we may see more on an ongoing basis. Employees or stakeholders who register a whistleblower complaint will be protected until the matter is resolved. SOx does seek to avoid frivolous complaints by requiring that the whistleblower must have a "reasonable" belief that the practice reported constitutes a violation.

Under these SOx rules, it is a crime for anyone "knowingly, with the intent to retaliate," to interfere with the employment or livelihood of any person—a whistleblower—who provides a law enforcement officer any truthful information relating to the possible commission of a SOx violation offense. Any whistleblower employee who then faces adverse employment action could potentially become a "protected informant" witness. Several legal sources have emphasized that this employee protection legislation is extraordinary and underscores the seriousness of these SOx rules.

SOx requires audit committees to establish a process for the receipt and treatment of complaints received regarding accounting, internal accounting controls, or auditing matters and for "the confidential, anonymous submission by employees" regarding questionable accounting or auditing matters. Stakeholders who believe they have been unlawfully discharged or discriminated against, due to their whistleblower action, may seek relief by filing a complaint, within 90 days after the date

of the violation, with the DOL or through initiating federal district court action. The aggrieved typically needs to secure legal help to seek relief, but numerous law firms will be eager to get involved. The process can be time consuming and expensive for the accused corporation. The procedural rules here, including the burdens of proof for the employer and employee, follow the Air 21 statute[2] for airline employees. For example, to prevail on a complaint before DOL, the employee must demonstrate that discriminatory reasons were a "contributing factor" in the unfavorable personnel action. Relief will be denied, however, if the employer demonstrates by "clear and convincing evidence" that it would have taken the same personnel action in the absence of protected activity.

An employee prevailing in such an action is entitled to full compensatory damages including reinstatement, back pay with interest, and compensation for the litigation costs and attorney fees. However, if DOL does not issue a final decision within 180 days of the whistleblower's complaint filing, the matter may be moved to the federal district court. Complicating matters further, the harmed whistleblower can take action on several fronts, seeking protection under federal and state laws as well as any collective bargaining agreement. Employers are exposed to potential "double jeopardy" for whistleblower actions with liability under both SOx and state or federal laws on wrongful discharge and similar causes of action. In addition, the aggrieved whistleblower can seek punitive damages through separate court actions.

Based on administrative and judicial experiences in the nuclear energy and airlines industries, whistleblower protection laws can become a potential enterprise minefield. If an employee raises any sort of accounting or auditing concern regarding an improper or illegal act, he or she is totally protected until the matter is investigated and resolved. There will be many trial lawyers eager to help the whistleblower and to file actions, particularly against major corporations with deep pockets. In addition, a substantial body of DOL and court precedent exists to support regulatory sanctions and personal remedies.

Based on over 20 years of experience with whistleblower protection laws, an impacted enterprise should attempt to strike a balance between the rights of employees to raise whistleblower concerns and the firm's ability to manage its workforce. A positive work environment is needed in which employees feel free to raise concerns to management coupled with effective mechanisms to deal with any concerns raised. The strong ethics-related programs discussed earlier in this chapter, including mission statements and codes of conduct, will support this strategy.

(b) SOx Whistleblower Rules and Internal Audit

As discussed, SOx whistleblower rules cover the reporting of an illegal or improper accounting, internal control, and auditing activity. This process becomes effective when, for example, the whistleblower is a member of the corporate accounting staff who hears of plans for some fraudulent transactions or an employee at a remote unit that is not frequently visited by corporate staff, such as internal audit. Whistleblower rules are designed to encourage stakeholders to report these fraudulent or illegal acts and very much to protect the person who reported the matter. This whistleblower reporting process raises some issues regarding internal auditors and their internal audit reviews.

An objective of internal auditing is to review and discover the types of accounting, internal control, and auditing issues specified in SOx. Internal audit findings

are reviewed with management and presented in a formal audit report where management can outline plans for corrective action. However, what if the internal audit team discovers an accounting, internal control, or auditing matter that is beyond the scope of the current audit and not formally reported in the audit report? Can one of the audit team members independently report the matter under SOx whistleblower procedures? Can an internal auditor who encounters a SOx accounting and internal control matter that is not part of a scheduled audit go through the whistleblower protection route to report the matter? What if the internal audit team member has not been performing well and fears termination? Can that poorly performing auditor dig up some potential findings, perhaps from past workpapers, and report them outside the audit department to obtain whistleblower protection and job security until the matter is resolved?

The internal audit team is clearly part of management, and the first responsibility of internal auditors is report any improper or illegal matters encountered during an audit to internal audit management for disposition. Internal audit team members should not attempt to work as independent whistleblowers as part of their internal audit work. Internal audit should develop a clear policy stating that any SOx accounting, internal control, or auditing matters encountered during the course of a scheduled audit review should be documented in the audit workpapers and communicated to internal audit management for resolution. Both the internal audit team and the management of the functions audited should understand that the purpose of internal audit is not to let loose a team of potential whistleblowers in a department's books and records. Any illegal or improper items should be investigated and reported through the normal internal audit process.

A situation could exist where an internal auditor does find some accounting or internal controls matter that gets somehow dropped from the audit process, perhaps in a senior auditor's workpaper review. The internal auditor has a first responsibility to get resolution on the matter up through the chief audit executive (CAE) or the audit committee. If the internal auditor documents and reports an issue, but internal audit management elects to drop or ignore it, the internal auditor then has the right and responsibility to report the matter to the enterprise's audit committee or even the SEC. Audit procedures and guidance should be in place to prevent such a frustrated internal auditor—potential whistleblower situation.

(c) Launching an Enterprise Help or Hotline Function

Many enterprises have help or hotline functions, administered through the ethics department, HR, or an independent provider, that allow any employee or stakeholder to call anonymously and either ask a question, report a concern, or blow the whistle on some matter. The idea is to provide an independent facility where all stakeholders can ask questions or report possible wrongdoings at any level. Hotline functions are not legally required but allow employees or other stakeholders to ask questions, to report possible wrongdoings, and even to seek advice. The items reported may range from allegations of theft of company property, HR complaints, or troubling questions. In most cases, the telephone operator will take all of the necessary information, asking questions when needed, and then pass the incident to an appropriate authority for investigation and resolution. The hotline operator typically assigns the reported incident a case number so the caller can later check on resolution.

Employee hotlines were established in many larger enterprises beginning in the mid-1990s. Often staffed with knowledgeable HR veterans who are skilled at answering HR-related issues, such as treatment in the workplace, these hotlines can be effective mechanisms to improve enterprise ethics and governance processes. When hotline calls include allegations of wrongdoing, the case should be shifted to others for investigation, such as to the legal department. In some instances, hotlines have turned into little more than corporate snitch lines where many minor gripes or infractions are reported; in general, however, hotlines have been very successful.

Many ethics hotlines were set up to be "friendly" in answering employee questions and giving some advice in addition to investigating reported incidents. Existing hotline programs must take a new approach when they also are used for the SOx whistleblower program, which emphasizes reporting improper financial accounting activities. While the more friendly help aspects of an ethics hotline can still apply, federal whistleblower rules require much more formal processes, particularly in areas such as confidentiality, documentation requirements for all records, and efficient processing of any investigations. In addition, the employee calling in a SOx whistleblower allegation is legally protected from any future recrimination. In some respects, no actions of any sort can be directed at that whistleblower by the employer until the allegation is resolved. There have been situations, under other federal whistleblower laws, where an employee who called in an issue had her desk moved and successfully brought legal action for whistleblower discrimination. There is no reason to establish separate ethics help lines and SOx whistleblower lines. Callers would be confused about which line to call. However, with the SOx whistleblower requirement, control procedures need to be enhanced in any established ethics hotline facility. Exhibit 24.3 contains guidelines for setting up a SOx whistleblower call center.

EXHIBIT 24.3 Guidelines for Setting Up a SOx Whistleblower Call Center

- Establish an independent—preferably toll-free—telephone line facility for the calls. The lines should not go through other enterprise switchboards.
- Train all operators in the facility with the basic provisions of federal whistleblower rules. Also, establish scripts such that call operators can respond and ask consistent general questions.
- Advertise and promote the facility throughout the enterprise: Emphasize that for all items reported, the caller eventually will be able to check status, all callers will be treated anonymously, and there will be no recrimination for caller actions.
- Implement a logging form to record all incoming calls. Maintain the date and time of the call, the caller's name or identification, and a summary of the details reported.
- Establish a routing and disposition process so that the status of who has the call information and the status of any investigation can be determined.
- Establish a secure database for all recorded whistleblower data with appropriate password protection.
- Working with the enterprise's human resource function, develop procedures to fully but anonymously protect all whistleblowers from recrimination of any sort.
- Develop processes for closing out all whistleblower calls and documenting all actions, if any.

The existence of an ethics hotline and whistleblower facility is of little value unless it is communicated and sold to all members of the enterprise. A good way to launch these processes is through the employee code of conduct, discussed previously. Even if such a hotline has already been launched, the fact that the line can be used for any potential SOx whistleblowers needs to be communicated. The goal should be to investigate and promptly resolve all calls—and especially whistleblower calls—internally to avoid outside investigators and lawyers.

24.4 Auditing the Enterprise's Ethics Functions

The ethics and hotline function should not be exempted from the same types of operational and financial reviews that internal audit performs in all other segments of the enterprise. Although the ethics function is different from asset management, marketing, or design engineering, which are subject to periodic operational or financial reviews based on potential audit risks, it should nevertheless be included in the same type of risk-analysis model discussed in Chapter 12. The ethics code of conduct function may introduce minimal risks, but the whistleblower function—particularly if it is administered internally—may present some major security and confidentiality risks. The CFO and other key officers are very much at risk if there are problems here.

The purpose of an internal audit review of the ethics and whistleblower function is to assess whether the ethics group is following good internal control procedures, making effective use of its resources, complying with good confidentiality procedures, and following its department charter authorizing the ethics function. Ethics and whistleblower functions may be a little different from company to company, but internal audit should gain a detailed understanding of how the function operates and the procedures normally performed. As the enterprise's *ethics function,* internal audit should expect to find procedures at least as good as internal audit regarding compliance with such areas as document confidentiality and with enterprise policies on travel expenses. Other ethics functions responsibilities may point to areas where internal audit can suggest improvements. For example, the ethics department's code of conduct normally should have an acknowledgment form or process whereby employees indicate that they have read and understand the code. An ethics function may not have established appropriate procedures here to ensure that all newly hired employees go through this code acknowledgment process. Internal audit can assess this process and recommend improvements where appropriate.

Exhibit 24.4 describes internal audit procedures for a review of an enterprise's ethics and whistleblower functions. Because of the close, ongoing relationship that should exist between the ethics function and internal audit, the CAE should discuss the planned review with the ethics director in some detail to explain the reasons for and the objectives of the review. Privacy and confidentiality may become an issue in this type of review. A call to the hotline may have pointed to some form of potential employee malfeasance or a SOx whistleblower revelation, which ethics will want to keep confidential until the matter is resolved. Despite internal audit's ongoing exposure to other sensitive areas and issues in the enterprise, the director of the ethics function may be reluctant to have internal auditors review certain materials. The CAE should point out internal audit's ongoing exposure to other sensitive information and the requirements that it follow appropriate professional standards.

EXHIBIT 24.4 Audit Steps for a Review of Ethics and Whistleblower Functions

1. Enterprise Mission Statements
   - 1.1. Review the enterprise's mission statement to assess whether is actively communicated and emphasizes the importance of governance and business ethics practices.
   - 1.2. If the mission statement appears to be lacking or in need of an update, discuss areas or plans for improvement with the audit committee.
   - 1.3. Meet with appropriate members of management to assess ongoing programs to promote the mission statement throughout the enterprise.
2. Ethics Function Administration
   - 2.1. Determine who has responsibility for administering the overall ethics program in the enterprise. Meet with the function to assess ongoing activities and programs.
   - 2.2. Develop an understanding and document the ethics function, including its structure and reporting relationships.
   - 2.3. Review the ethics function's charter and other key process documentation, and determine that they are consistent with other enterprise initiatives.
   - 2.4. Determine whether there is some form of hotline function in place, and assess its span of activities.
   - 2.5. Assess the ethics function office security procedures for the adequacy of records, files, and workstation security.
   - 2.6. If outside contractors are used to provide ethics or hotline services, review and document contractual arrangements.
3. Code of Conduct Processes
   - 3.1. Obtain a copy of the current code of conduct.
     - 3.1.1. Determine that the code is current and regularly updated.
     - 3.1.2. Discuss the code with a sample on enterprise staff to determine that they understand the code document.
     - 3.1.3. Discuss the code with selected managers at all levels to determine if there are concerns about the code's issues or content.
   - 3.2. Assess the adequacy of processes for obtaining code acknowledgments.
     - 3.2.1. Select a sample of employees and determine that they acknowledged acceptance of the code.
     - 3.2.2. Determine that all officers have accepted the code.
     - 3.2.3. Assess adequacy of procedures for any employees who fail/refuse code acknowledgment.
     - 3.2.4. Assess the adequacy of code acknowledgment records.
   - 3.3. Assess the adequacy of processes for updating the code of conduct as required.
   - 3.4. Assess processes in place to distribute code to all enterprise stakeholders, including remote locations such as foreign, vendors, and others.
4. Hotline/Whistleblower Processes.
   - 4.1. Develop a general understanding of whistleblower processes in place, and determine that they cover audit committee SOx requirements.
   - 4.2. Assess the adequacy of procedures to communicate the whistleblower program to all stakeholders.
   - 4.3. Assess the adequacy of processes for logging whistleblower messages or calls received and documenting interactions.
   - 4.4. Review the process for disposition of calls, and select a sample of recent calls to determine if processes appear adequate.
   - 4.5. Review overall security processes in place, including protection of key documents and individual whistleblower stakeholders.
   - 4.6. Meet with human resources to determine that adequate procedures are place to protect/encapsulate any whistleblowers.
5. Audit Committee Responsibilities. Meet with the audit committee representative to determine knowledge and understanding of the ethics and whistleblower programs in place.

Assuming these matters can be resolved appropriately, an operational review of an ethics function will give management additional assurances as to the integrity of controls in the ethics function, a component of operations where most managers have had little exposure or experience.

24.5 Improving Corporate Governance Practices

A strong ethics program, based on a meaningful mission statement and a code of conduct, is a key element in any overall program of corporate governance in the enterprise. The accounting scandals that led to SOx were, in many respects, scandals at the top levels of the enterprise, whether caused by a scheming financial officer, a greedy CEO, or a don't-ask-any-questions public accounting firm. The executive teams at the accounting scandal companies set their own rules with little consideration given to the rest of the enterprise. As a result, SOx is particularly focused on this senior group. However, an overall strong ethics program will improve corporate governance practices for the entire enterprise, not just the people in the executive office.

As part of their role as the ethics leaders in their enterprise, internal auditors should be very aware of the need for overall enterprise-wide corporate governance and ethics policies. Internal auditors should have strong ethics and compliance programs in place within their own internal audit group and should look for similar practices within the total enterprise. These practices include enterprise senior management policy statements to emphasize that all stakeholders are encouraged, indeed have an obligation, to bring concerns about accounting and financial practices to the attention of management. Such policy statements should also stress that management will not tolerate retaliation against employees who raise concerns. The policy can help foster an open-door process for addressing issues, which, after all, is the most effective management approach.

The ethics and whistleblower processes discussed in this chapter are important both for SOx compliance and good corporate governance practices, no matter what the size of the organization. Internal auditors should be aware of these practices as part of their CBOK and should play a key role in helping both to launch and to review these processes.

Notes

1. At that time, the Internet was first introduced as a potentially powerful business tool and many companies were launched to try to exploit its potential. Many were ill-conceived and eventually failed.
2. The Wendell H. Ford Aviation Investment and Reform Act for the 21st Century (commonly known as Air 21) protects whistleblowers in the airline industry. A related act is the 1978 Energy Reorganization Act, which protects employees in the nuclear power industry from retaliation for their reporting of safety concerns.

CHAPTER 25

Fraud Detection and Prevention

Seemingly like clockwork, enterprises in the United States and elsewhere regularly go through periods when there are many business failures; often they are based on economic conditions, but sometimes on questionable business activities or just fraud. For example, the financial scandals at Enron and others that led to the enactment of the Sarbanes-Oxley Act (SOx) were examples of financial fraud by senior corporate officers. Fraudulent activity can occur at all levels of the enterprise, but in mid-2002, around the time of the enactment of SOx, corporate officers appeared to be the real troublemakers in a slew of financial frauds. Just as a chief executive officer (CEO), in cooperation with the chief financial officer (CFO), may fraudulently manipulate earnings to boost reported profits and their bonus compensation, a midlevel manager or even a staff-level employee may initiate some fraudulent action for personal gain or just to get even with someone because of job frustration. Unfortunately, the publicity surrounding Enron and other incidents of fraud at that time created an almost everybody-does-it attitude in recent years. Ernst & Young in its 2003 Global Fraud Survey[1] reports that 85% of the worst frauds were caused by insiders on the payroll, and over half of those frauds were initiated by members of management. SOx and its strong emphasis on better internal controls did not change things. Early 2004 brought the $18 billion Parmalat fraud covering—of all things—a dairy company headquartered in Parma, Italy, that primarily distributed milk. The fraud was based on a large number of fictitious accounts with huge amounts of money siphoned off to the perpetrators. An effective internal auditor needs to recognize potential fraudulent business practices as part of any audit and then should recommend controls and procedures to limit exposure to the fraudulent activity. This chapter outlines some of the red flags—common conditions that an internal audit might encounter when faced with a potential fraud. The chapter then discusses steps to identify, test, and properly process fraudulent activities. We also discuss fraud-related auditing standards both from the perspective of the Institute of Internal Auditors (IIA) standards as well as U.S. external auditing fraud investigation standards. In addition, the chapter introduces the standards and activities of the Association of Certified Fraud Examiners (ACFE). Fraud investigation can be a very detailed and specialized activity, but all internal auditors should have at least a high-level common book of knowledge (CBOK) understanding of how to "smell" potentially fraudulent circumstances, how to audit for fraudulent activities, and processes for investigating and reporting fraud. Fraudulent activities represent a breakdown in a wide range of good practices and procedures, but internal auditors must recognize that these activities always may exist.

25.1 Understanding and Recognizing Fraud

Fraud is one of those terms that many people often use even though they do not fully understand what they are talking about. An important internal auditor first step here should be to understand the dictionary or legal definition of what we call fraud. Its common law definition is the obtaining of money or property by means of false token, symbol, or device. In other words, someone improperly authorizes some document that causes an improper transfer of money. Fraud can be costly for any victim enterprise, and effective internal controls are an enterprise's first line of defense against fraud. A comprehensive, fully implemented, and regularly monitored system of internal controls is essential for the prevention and detection of losses that arise from fraud, and internal auditors often find themselves very involved in fraud-related issues. When a fraud is discovered in the enterprise, internal audit is often the first resource called to conduct an investigation to determine the extent of the reported fraud. In other situations, internal auditors discover a fraud during a scheduled audit and then investigate and report the matter to their corporate consul or other legal authorities. However, historically, both internal and external auditors have not regularly looked for fraud as part of their scheduled audits. This is changing.

Auditors today, both internal and external, are taking on a more important role in the detection and prevention of fraud. This chapter discusses controls to prevent and detect fraud and introduces the American Institute of Certified Public Accountants (AICPA) auditing standard on fraud, Statement on Auditing Standards (SAS) No. 99, *Consideration of Fraud in a Financial Statement Audit.* While the SAS series of auditing standards has essentially gone away with the enactment of SOx and its Public Corporation Auditing Oversight Board (PCAOB), SAS No. 99 was a last[2] but very important auditing standard prior to SOx. This chapter also discusses IIA initiatives to review for fraud in internal audits as well as procedures to detect and prevent computer systems fraud. Fraud has been with us from time immemorial, but in the past many auditors have claimed that detecting fraud was beyond their responsibilities. Today, they are finding themselves with an increasing responsibility to detect fraud in the course of their review activities as well as to recommend appropriate controls to prevent future frauds. As this book goes to press, joint guidance material on the impact of fraud in auditing has been released by a task force from the AICPA, the IIA, and the ACFE.[3] While still in draft form, such guidance highlights the importance of fraud considerations for internal auditors and others.

25.2 Red Flags: Fraud Detection Signs for Internal Auditors

Many fraudulent activities are easy to identify *after the fraud has been uncovered.* An employee of an enterprise who has been embezzling money over an extended period often eventually is caught through some slip-up that reveals the employee's fraud. After such a fraud is discovered, it is easy to look at the situation and say, "But, she was such a good employee—she has not missed a day of work for nearly two years! How could she have done this?" or "Now that I think about it, I wondered how he could afford all of those long weekend trips to expensive places!" It is easy to analyze the facts after a fraud has been discovered as a "lesson learned," but

auditors and management should look for indicators of possible fraudulent activities in advance. They should look for what are called red flags.

For example, the first corporation and CEO to be indicted for accounting fraud under SOx was a healthcare provider called HealthSouth Corporation. Then the largest U.S. provider of outpatient surgery, diagnostic, and rehabilitative services, HealthSouth operated in approximately 1,900 locations in 50 states as well as multiple international facilities. It reported in excess of $1.4 billion of *fictitious* earnings over a six-year period in order to meet investment analyst estimates and to keep its stock price high. Several of its financial and other officers pleaded guilty, claiming and testifying against the CEO and asserting that he demanded they report the fraudulent earnings. This accounting fraud had been happening over a period of at least some 10 years at that time, and there had been numerous red flags of possible fraud that were seemingly ignored by their external auditors and others:

- HealthSouth's year 2000 pretax earnings more than doubled to $559 million, although its sales grew only 3%. Pretax earnings for 2001 were nearly twice 1999 levels, although sales rose just 8%. While there is nothing wrong with fantastic earnings growth, analysts and certainly auditors might have asked some hard questions.
- In late 2002, HealthSouth's internal auditors were denied access to key corporate financial records. Internal audit reported this to their outside auditors and to the audit committee; neither party took any action on these internal audit concerns.
- The CEO spent a considerable amount of time and attention on sports and popular music performers, flying his management staff off to events and bringing sports stars in to work with the company.

These are just a few examples of the activities that were occurring at HealthSouth that suggest possible fraud. Fantastic percentage reported earnings gains does not mean fraud but can raise questions. Similarly, elaborate corporate-sponsored social events may raise questions about how the enterprise is managing its resources rather than pointing to fraud. At HealthSouth, an ex-employee even sent an e-mail to the external auditors suggesting they look at three specific accounts for fraudulent activity. This is more than a red flag; it is an attempt to blow the whistle. Based on this tip, a high-level investigation was launched by the external auditors but nothing was found. There were many red flags raised here, but internal management pressure on a normally dominant CEO to back off from some fictitious financial reports eventually started a chain of events that exposed the fraud.

What we call a red flag here is a warning signal to the noninvolved observer that something does not look right. A huge increase in reported profits with not that much of an increase in unit sales may sound wonderful and be totally plausible. However, when faced with this type of red flag indicator, auditors or fraud examiners should say, "This seems unusual—how can it be so?"

Red flags are normally the first indications of a potential fraud. Someone sees something that does not look right and often begins a low-level investigation. Internal auditors are often the very first people to become involved. Exhibit 25.1 lists some typical red flag signs that could point to potential financial fraud activities. None of these is an absolute indicator of fraud, but internal auditors should always be

EXHIBIT 25.1 Red Flags Indicating Potential Financial Fraud

- Lack of written corporate policies and standard operating procedures.
- Based on interviews at multiple levels, lack of compliance with organization internal control policies.
- Weak internal control policies, especially in the division of duties.
- Disorganized operations in such areas as purchasing, receiving, warehousing, or regional offices.
- Unrecorded transactions or missing records.
- Counterfeit or evidence of alterations to documents.
- Photocopied or questionable handwriting on documents.
- Sales records with excessive voids or credits.
- Bank accounts not reconciled on a timely basis or stale items on bank reconciliations.
- Continuous out-of-balance conditions on subsidiary ledgers.
- Unusual financial statement relationships.
- Continuous unexplained differences between physical inventory counts and perpetual inventory records.
- Bank checks written to cash in large amounts.
- Handwritten checks in a computer environment.
- Continuous or unusual fund transfers among company bank accounts.
- Fund transfers to offshore banks.
- Transactions not consistent with the entity's business.
- Poor screening procedures for new employees, including no background or reference checks.
- Reluctance by management to report criminal wrongdoing.
- Unusual transfers of personal assets.
- Officers or employees with lifestyles apparently beyond their means.
- Unused vacation time.
- Frequent or unusual related-party transactions.
- Employees in close association with suppliers.
- Employees in close relationship with one another in areas where separation of duties could be circumvented.
- Expense account abuse such as managers not following established rules.
- Business assets dissipating without explanation.

Source: Adapted from the AICPA Web site, aicpa.org.

skeptical in their reviews and be aware of such warning signals. When an internal auditor sees evidence of one or more of these or other red flags, it may be time to dig a little deeper.

Unfortunately, internal auditors often fail to detect frauds for one of these reasons:

- **Unwillingness to look for fraud.** Based on their training and past experience, internal auditors historically have not actively looked for fraud. Often they tend to view fraud investigation as a police detective type of activity, not a prime internal audit responsibility.
- **Too much trust is placed on auditees.** Internal auditors, usually, try to maintain a friendly, cordial attitude toward auditees in their enterprise. Because they encounter these same people in the cafeteria or at an annual company picnic,

usually a level of trust exists. Internal auditors quite correctly try to give their auditees the benefit of the doubt.

- **Not enough emphasis is placed on potential fraud issues in audit findings** Internal audit findings often point to some of the same red flags as mentioned in Exhibit 25.1. They are included as audit report findings pointing out such matters as missing records or accounts that were not reconciled. However, internal auditors often do not consider potential fraud in audit findings. Unless it is a glaringly large issue, internal auditors do not even consider fraud issues when developing such an audit report finding.
- **Fraud concerns receive inadequate support from management.** The hint of possible fraud requires auditors to extend their procedures and often dig a lot deeper. However, general and even audit management may be reluctant to give an individual auditor extra time to dig deeper. Unless there are strong suspicions to the contrary, management often wants the audit team to move on and stop spending time in what they often feel is an extremely low risk area.
- **Auditors sometimes just fail to focus on high-risk fraud areas.** Fraud can occur in many areas, ranging from employee travel expense reporting to treasury function relations with offshore banks. Often a much greater risk exists in the latter areas, although auditors often focus on the former ones. It may be comparatively easy to find problems in travel expenses. Internal audits often does not include such high-risk areas as the example review of treasury function relations with offshore banks. Chapter 15 on risk-based audit planning highlights this issue; we often fail focus scheduled audits on areas with high fraud potential.

The word *fraud* can have many meanings, but we are referring to it as a criminal act. There are over 300 references to fraud in federal criminal statutes, and the term appears throughout the actual SOx legislation. Most of those federal references are based on federal general fraud statute, which reads:[4]

> *Whoever, in any manner within the jurisdiction of any department or agency of the United States, knowingly and willfully falsifies, conceals, or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious, or fraudulent writing or document knowingly the same to contain any false, fictitious, or fraudulent statement or entry, shall be fined not more than . . . or imprisoned not more than . . . or both.*

This statement, though framed in legalese, is a strong one. The auditor's word *material* is not included here; thus anything false, fictitious, or fraudulent could be considered a violation. Numerous state statutes are generally modeled after these federal rules, and an internal auditor should be aware of his or her state rules.

To help detect fraud, auditors need to have an understanding of why people commit fraud. An enterprise can have the red flag environment described in the previous section, but it will not necessarily be subject to fraudulent activities unless one or more employees decide to engage in fraud. Exhibit 25.2 lists some typical reasons or excuses for committing a fraud. These are all reasons where strong

EXHIBIT 25.2 Excuses and Reasons for Committing Fraud

- **An employee has desperate need for money.** This probably is the major motivator and the fraud most difficult to detect. Whether due to a nasty divorce or a drug problem, the need for money can cause employees to resort to criminal actions.
- **Job frustrations.** Employees who are frustrated and feel their company "doesn't give a damn" about them may feel free to act inappropriately. Job layoffs or pay grade freezes can foster such feelings.
- **Everybody does it attitudes.** This type of situation is common in small retail-type environments where an employee thinks that everyone else is stealing. This attitude can also come up when senior managers seem to be living extravagantly at the same time the company is incurring losses.
- **Challenges to beat the system.** This is a particular problem with would-be hackers in an automated systems environment. However, there can be many other cases where an employee tries to set up a fictitious account to see he can bill the company and receive cash in return, for example.
- **Lax internal controls making fraud easy.** This is a basic motivation that encourages many frauds. Poor internal controls often predict that the fraud will not be detected.
- **Low probability of detection** . Similar to the weak internal controls point, if an employee knows that chances of getting caught are nil, the temptation to commit fraud is greater.
- **Low probability of prosecution** . When a company seemingly never takes any action to bring criminal charges against someone, the word gets out, and people may view getting caught as an acceptable risk with little worry about prosecution.
- **Top management that does not seem to care** . Employees often collectively determine when an employee seems to get away after breaking some rule or when otherwise appropriate behavior is not rewarded.
- **Low organizational loyalty or feelings of ownership** . In today's complex world, the owners of a business operation may be a continent and many organizational layers away. In these cases, it is easy for attitudes of no one seeming to care to develop.
- **Unreasonable budget expectations or other financia targets** . Organizations sometimes establish expectations that are all-but-impossible to meet. This can create an environment where people will bend the rules to meet those targets.
- **Less-than-competitive compensation and poor promotion opportunities** . If they cannot receive what they feel are appropriate rewards through normal compensation, people may bend the rules to benefit themselves.

internal controls are in place and the fraud is committed by one person only. Fraud detection is much harder when there is collusion between multiple persons. In the HealthSouth fraud described previously, a very aggressive CEO assembled a top management team he called "the company" to prepare the fraudulent financial reports. Members of "the company" were highly compensated and received many incentives. The fraud did not become public until a member of "the company" began to have personal concerns about this growing accounting fraud. Whenever multiple people are in same fraud together, there is always a possibility that someone will break ranks.

Major frauds involving senior management participation are difficult to detect; those that occur at lower levels in the enterprise are often easier to detect with a proper level of internal auditor investigation. For example, a payroll process can present a wide range of opportunities for fraud through the use of such

mechanisms as inflating the actual hours worked for an employee, generating payment vouchers for fictitious or terminated employees, or issuing duplicate vouchers for an employee. These are the classic types of issues that are part of many internal audit procedures. However, rather than just an internal control violation, an internal auditor should think of these items in terms of potential areas for employee fraud. Auditors have performed these procedures for years but sometimes forget that there could be a fraud issue as well. In the HealthSouth fraud just discussed, it was later discovered that the external auditors did not even do a classic account confirmation with HealthSouth's banks. A bank balance conformation is a standard test where the auditor asks the bank independently to confirm an audited entity's bank balance as of a certain date. The Parmalat fraud included fraudulent bank confirmation letters that probably could have been detected sooner if the auditors had looked a bit harder. In their promotion of audit efficiency over the years, auditors—particularly external auditors—have dropped many of these traditional audit procedures. It may be time to revisit some.

25.3 Public Accounting's Role in Fraud Detection

The external auditor's responsibility for the detection of fraud in financial statements has been an ongoing but contentious issue over the years. The very first AICPA Statement on Auditing Standards (SAS No. 1) from many years ago stated:

> *The auditor has no responsibility to plan and perform the audit to obtain reasonable assurance that misstatements, whether caused by errors or fraud, that are not material to the financial statements are detected.*

In other words, at the time, external auditors were responsible only for determining if the financial statements were fairly stated; they had *no responsibility* to detect errors or fraudulent activity. The public accounting profession stood by this position for many years. Even during the period of numerous financial frauds that led to the 1987 Treadway Commission Report on Fraudulent Financial Reporting (see Chapter 3), AICPA audit standards still did not require external auditors include to assume any responsibility for the detection of fraud

Despite continuing pressure over the years for change, AICPA audit standards regarding the external auditor's responsibility for fraud did not change until 1997, when this responsibility for fraud was restated in SAS No. 82: "The auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud." This revised but tighter standard was released, after much professional discussion, at the peak of the dot-com bubble, when the investing public was concerned about investments surging forward and not that much with fraud.

Early in the twenty-first century, with the failures of Enron, WorldCom, and a host of others, concerns about fraudulent financial reporting changed. Given SOx and the new PCAOB, it was perhaps now too late, but in December 2002 the AICPA released SAS No. 99 on the auditor's responsibility for detecting fraudulent financial reporting. With this auditing standard, an external auditor is now responsible for providing reasonable assurance that audited financial statements are free of material

misstatement, *whether caused by error or fraud*. We have used italics here, because SAS No. 99 was a major change in external auditor responsibilities.

SAS No. 99 calls on external financial statement auditors to take on an attitude of professional skepticism regarding possible fraud. Putting aside any prior beliefs as to management's honesty, the standard calls for the external audit team to exchange ideas or brainstorm on how frauds could occur in the enterprise they are about to audit. These discussions should identify fraud risks and should always keep in mind the characteristics that are present when frauds occur: incentives, opportunities, and ability to rationalize. Throughout the audit, the engagement team should think about and explore the question: If someone wanted to perpetrate a fraud here, how would it be done? From these discussions, the external audit team should be in a better position to design audit tests that are responsive to the risks of fraud. The guidance here is that the external audit team should *always* go in to an audit engagement anticipating that there may be some level of fraudulent activity.

The external auditor engagement team now is expected to ask management and others in the enterprise regarding their perceptions of the risk of fraud and whether they are aware of any ongoing fraud investigations or open issues. The external auditors should make a point of talking to all levels of employees, both managers and others, giving them an opportunity to blow the whistle and encouraging someone to step forward. Concern that a coworker may turn them in during a subsequent audit might help deter a person from committing fraud. During an audit, the external audit engagement team should test areas, locations, and accounts that otherwise might not be tested. The team should design tests that would be unpredictable and unexpected by the client. This represents a major change in external auditing standards.

SAS No. 99 also recognizes that management is often in a position to override controls in order to commit financial statement fraud. The auditing standard calls for procedures to test for potential management overrides of controls on every audit. SAS No. 99 calls for a major external audit emphasis in detecting fraud, including procedures that external auditors are expected to perform in every audit engagement. This can be a major change from the "Let's take the afternoon off and talk about things over a game of golf" approach that was common in many past external audit engagements.

In addition to imposing a very tough fraud detection auditing standard on its members, the AICPA now has taken strong steps to bring external auditors up to speed regarding situations that encourage fraud as well as providing both educational materials and case studies. Its Web pages are filed with case studies, publications, continuing professional education (CPE) courses, and other references on management fraud issues. You do not have to be an AICPA member to access the site, and there are member and nonmember prices for purchasing reference materials. As an example of the AICPA fraud-related materials, Exhibit 25.3 shows a misappropriation of assets checklist for auditors. Although the AICPA avoided getting involved in fraud prevention and detection work for many years, its SAS No. 99 standards and its published antifraud guidance materials very much raise the bar for all certified public accountants (CPAs). It is unfortunate that these audit standards were not released sooner.

Internal auditors will be seeing more fraud-related audit guidance going forward. As this book was going to press, the AICPA, the IIA, and ACFE released an exposure draft, "Managing the Business Risk of Fraud: A Practical Guide."[5] Some of these concepts are included in our internal auditor guidance here.

EXHIBIT 25.3 Fraud Risk Factors Relating to Misappropriation of Assets

Risk factors that relate to misstatements arising from misappropriation of assets are classified according to the three conditions generally present when fraud exists: (1) incentives/pressures, (2) opportunities, and (3) attitudes/rationalizations. Some of the risk factors related to misstatements arising from fraudulent financial reporting also may be present when misstatements arising from misappropriation of assets occur. For example, ineffective monitoring of management and weaknesses in internal control may be present when misstatements due to either fraudulent financial reporting or misappropriation of assets exist. The following are examples of risk factors related to misstatements arising from misappropriation of assets.

Incentives/Pressures

A. Personal financial obligations may create pressure on management or employees with access to cash or other assets susceptible to theft to misappropriate those assets.
B. Adverse relationships between the entity and employees with access to cash or other assets susceptible to theft may motivate those employees to misappropriate those assets. For example, adverse relationships may be created by the following:
   - Known or anticipated future employee layoffs
   - Recent or anticipated changes to employee compensation or benefit plans
   - Promotions, compensation, or other rewards inconsistent with expectations

Opportunities

A. Certain characteristics or circumstances may increase the susceptibility of assets to misappropriation. For example, opportunities to misappropriate assets increase when there are the following:
   - Large amounts of cash on hand or processed
   - Inventory items that are small in size, of high value, or in high demand
   - Easily convertible assets, such as bearer bonds, diamonds, or computer chips
   - Fixed assets that are small in size, marketable, or lacking observable identification of ownership
B. Inadequate internal control over assets may increase the susceptibility of misappropriation of those assets. For example, misappropriation of assets may occur because there is the following:
   - Inadequate segregation of duties or independent checks
   - Inadequate management oversight of employees responsible for assets (for example, inadequate supervision or monitoring of remote locations)
   - Inadequate job applicant screening of employees with access to assets
   - Inadequate recordkeeping with respect to assets
   - Inadequate system of authorization and approval of transactions (for example, in purchasing)
   - Inadequate physical safeguards over cash, investments, inventory, or fixed assets
   - Lack of complete and timely reconciliations of assets
   - Lack of timely and appropriate documentation of transactions (for example, credits for merchandise returns)
   - Lack of mandatory vacations for employees performing key control functions
   - Inadequate management understanding of information technology, which enables information technology employees to perpetrate a misappropriation
   - Inadequate access controls over automated records, including controls over and review of computer systems event logs.

Source: Printed with permission of the American Institute of Certified Public Accountants.

25.4 IIA Standards for Detecting and Investigating Fraud

Internal auditors are often in a better position to detect fraud than external auditors. External auditors limit most of their client visits to around the quarterly and annual financial statement dates; internal auditors are just that—internal to the enterprise and at enterprise sites on a daily basis. Just through observation, an internal auditor may be in a much better position to see a red flag that an external auditor could easily miss, despite the new AICPA fraud standard. The shipping supervisor who shows up at the annual holiday party in an expensive Italian suit and sporting a brand-name gold wristwatch might raise a small blip on the radar screen of another party participant, an internal auditor. There are many very valid reasons to justify expensive clothes, but such a show of wealth could be something for an internal auditor to remember going forward with an internal audit scheduled in that area.

Internal auditors run into many such concerns and potential fraud issues in the course of scheduled reviews. They also typically get involved in much more detailed, transaction-level reviews than their external audit counterparts and see questionable documents or transactions more frequently. If management feels there may be a potential fraud in the enterprise, the first step is almost always to contact internal audit, who also will have some connection and communication with the corporate legal department. The legal department can discuss any potential concerns there and give internal audit a quick opinion whether some concern requires more attention. If there are strong signs of an active fraud, corporate legal will almost always be ready to jump in and help.

The IIA standards emphasize that internal audit has a role to play regarding fraud detection and prevention, but the primary fraud detection responsibility falls on management. Although this sounds simple in theory, the problem lies in communicating that message to management. IIA *International Standards for the Professional Practice of Internal Auditing* covering due professional care and scope of work, as discussed in Chapter 8, cover fraud in only a very general sense. An internal auditor should be concerned about such matters as the possibility of wrongdoing and also should look for any evidence of any improper or illegal activities in an audit. However, the IIA standards that provide specific guidance on fraud seem to follow the older external audit standards just discussed. Recognizing that it may be difficult to detect fraud, the revised 2004 IIA standard 1210.A2 states, with our italics noted: "The internal auditor should have sufficient knowledge to identify the indicators of fraud *but is not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud*." This is a recognition that internal auditors may not have the expertise for fraud issues.

This same fraud standard is supported by an IIA Practice Advisories 1210.A2–1 and -2, on the identification and investigation of fraud. Despite the words that internal auditors are *not expected to have the expertise* from the standard, the supporting Practice Advisory provides an internal auditor with some guidance on detecting and investigating fraud.

Internal auditors are responsible for assisting in the deterrence of fraud by examining and evaluating the adequacy and effectiveness of the system of internal control, commensurate with the extent of the potential exposure/risk in the various

segments of the enterprise's operations. In carrying out this responsibility, internal auditors should, for example, determine whether:

- The organization's environment fosters control consciousness, and realistic enterprise goals and objectives are set.
- Written policies (e.g., codes of conduct) exist that describe prohibited activities and the action required whenever violations are discovered.
- Appropriate authorization policies for transactions are established and maintained.
- Policies, practices, procedures, reports, and other mechanisms are developed to monitor activities and safeguard assets, particularly in high-risk areas.
- Communication channels provide management with adequate and reliable information.
- Recommendations need to be made for the establishment or enhancement of cost-effective controls to help deter fraud.

When an internal auditor suspects a potential fraudulent activity, appropriate enterprise authorities, such as the legal department, should be informed. The internal auditor may recommend whatever investigation is considered necessary in the circumstances. Thereafter, the auditor should follow up to see that the internal auditing activity's responsibilities have been met.

These Practice Advisories do not really educate an internal auditor on red flag types of conditions that might suggest potential fraudulent activity. Rather, they suggest that if an enterprise does not have good policies and procedures or lacks a code of conduct, this could indicate an environment that encourages fraud. This is often true. But the lack of a current code of conduct or poorly drafted policy statements should not be the major reason for an internal auditor to go on a hunt to for potential fraudulent activities. The red flags of Exhibit 25.1 are better indicators.

The IIA has not taken the strong position on detecting fraud that the AICPA has. A mid-2008 search to the IIA Web site using the key word *fraud* does not give an auditor the wealth of material found on the AICPA site. There are references to articles on fraud in older issues of the IIA publication, *The Internal Auditor,* but not much more. Other fraud-related articles are listed but available only to IIA members. The previously referenced two Practice Advisories are examples. The IIA also has special conferences on the topic, but the AICPA seems to be taking a stronger professional lead here in providing fraud auditing guidance to auditors.

The IIA along with the AICPA, Information Systems Audit and Control Association, the ACFE, Financial Executives International, Institute of Management Accountants, and the Society for Human Resource Management have collaborated and sponsored a set of fraud guidance materials published as a supplement to SAS No. 99. Other professional enterprises that have participated in reviewing and developing fraud guidance include the American Accounting Association, Defense Industry Initiative, and the National Association of Corporate Directors. However, the AICPA is clearly taking a lead role here, and internal auditors should visit the AICPA Web site (www://aicpa.org/antifraud/homepage) for more information.

25.5 Fraud Investigations for Internal Auditors

In addition to helping to build and review controls to prevent and detect fraud, internal auditors sometimes become very involved in fraud investigations. While appropriate legal authorities should be used here for many fraud investigations, internal audit often can play a key role in other, less major matters. Internal auditors should generally not play the role of a Sherlock Holmes here but can help to gather information for smaller discovers or provide supporting materials for larger matters. Internal audit often gets involved in potential fraud-related matters because of some troubling information encountered during an audit or an anonymous tip through a call or e-mail note.

When faced with such potential fraud information, internal audit's first step should always be to consult with the enterprise's corporate counsel. Because of the nature of the allegation as well as the extent of initial information, the matter may be turned over to legal authorities, such as the federal district attorney's office or state prosecutors. In some cases, legal advice will suggest that other authorities get involved in the matter at once. In smaller, seemingly less major matters, internal audit will sometimes be asked to take responsibility for the investigation. Many times these types of investigations involve detailed reviews of documents. The evidence gathered from those document reviews becomes the basis for any further action to be taken.

Fraud related investigations require an internal auditor to operate rather differently. In any fraud-related review, an auditor should have three major objectives:

1. **Prove the loss.** Fraud-related reviews usually start out with the finding that someone stole something. The internal audit–led investigative review should assemble as much relevant material as necessary to determine overall size and scope of the loss.
2. **Establish responsibility and intent.** This is a "Who did it?" step. As much as possible, internal auditors should attempt to identify all parties responsible for the loss and if there are any special or different circumstances associated with the fraud action.
3. **Prove the audit investigative methods used.** The investigative team needs to be able to prove that its fraud-related conclusions were based on a detailed, step-by-step investigative process, not just an uncoordinated witch hunt. The review should be documented using the best internal audit review processes. Of particular importance here, all documents used need to be secured.

There are many other procedures associated with a fraud-related examination. The objective of this book is not to describe the overall process of fraud examinations but to discuss the increased emphasis on fraud detection and prevention as outlined by new standards, particularly the AICPA SAS No. 99, as well as the IIA fraud management publications currently in draft form. Internal auditors interested in learning more about fraud investigations should explore the activities and publications of the ACFE (www.cfenet.com). This professional enterprise has a wide variety of fraud-related educational and guidance materials.

25.6 Information Technology Fraud Prevention Processes

Information technology (IT) or technology-related fraud covers a wide range of issues and concerns. In today's business environment, information systems are virtually always a key component of any modern financial or accounting-related fraud. Because IT systems and processes support so many areas and cross so many lines in the enterprise, we can think of IT-related fraud in multiple dimensions ranging from the minor to significant fraudulent activities:

- **Internet access issues.** Enterprises often establish both guidelines and sometimes controls to restrict Internet use, but the Web is so pervasive that it is difficult to separate personal from business use. Again, such rules frequently are ignored by employees and sometimes bypassed by the use of software that will allow them to get around firewall barriers in systems. There can be a strong possibility of abuse here, but also the enterprise can monitor employee Internet usage through software monitoring tools. Many may wink at such matters, but an enterprise associate should not be spending substantial amounts of workday time browsing through the Internet or completing home shopping transactions.
- **Improper personal use of IT resources.** An enterprise should establish rules stating that there should be no personal files or programs on work-supplied systems. Employees frequently ignore such rules, and may use word processing or spreadsheet resources to perform some personal work both in the office and at home. An enterprise should emphasize to employees that they should not be doing personal business while at the workplace. Perhaps even greater than the risk of fraud here is the possibility of introducing viruses or other harmful software to enterprise systems.
- **Illegal use of software.** Employees sometimes attempt to steal/download copies of company software or install their own software on enterprise computer resources. By doing so, they are violating enterprise rules and often putting their employers in violation of software license agreements. In addition, they may be potentially introducing viruses into enterprise systems. While an enterprise should have systems firewalls installed to protect itself from such improper software, there is always to risk of such malignant software slipping through.
- **Computer security and confidentialit fraud matters.** Employees can violate password protections and gain improper access to computer systems and files. Even if they are only trying to see if it works, they are performing a fraudulent act by violating computer security rules.
- **Information theft through USB devices.** Today, storage devices about the size of an auto ignition key can be plugged into a computer system and used to download multiple gigabytes[6] of information. An enterprise can face a significant risk of the theft or loss of such data as customer records through these simple storage management devices.
- **Information theft or other data abuse computer fraud.** It is one thing to improperly access a computer system by violating password controls and another to improperly view, modify, or copy data or files. This can be a significant cause of computer crime.

- **Embezzlement or unauthorized electronic fund transfers.** Stealing money or other resources through improper or unauthorized transactions is the most significant cause of IT systems and network fraud issues. Whether initiating a transaction to send an accounts payable check to the home address or facilitating a major bank transfer, this can be a major area for computer fraud or crime.

These examples run the course from what might be considered fairly minor to significant IT abuses. We mention the more minor items to point out the range of things that can be considered computer fraud. If an employee is given a laptop computer for work and told it is only for business use, but if the employee uses that same laptop to write a book report as part of her child's homework, does this represent computer crime or fraud? The answer here is really yes, per the established rules. If an enterprise sets up rules, they are established for good reason, and employees should not violate them. However, should internal audit launch a review to discover violations in this area? Probably not; there are more important high-risk areas on which to spend limited time and resources. A strong code of conduct and ethics program, as discussed in Chapter 24, should be the predominant control procedure here.

We have used the book report example to illustrate that there are many possibilities for computer fraud and abuse. It is often also a very complex area where strong technical skills are needed to understand tools and methods. This is an area where the rules are changing continually. Individuals with a fraudulent intent are finding new ways to violate established automated controls, and skilled professionals are finding ways to detect and protect this fraudulent activity. Chapter 20 discusses IT security and privacy controls in a networked environment.

A related computer systems fraud detection area is computer forensics, the detailed examination of computers and their peripheral devices, using computer investigation and analysis techniques for finding or determining potential legal evidence in a fraud situation. The idea here is that essentially anything written on a computer file can be recovered, even if it has been erased through an operating system command. The evidence to be found covers a wide range of subjects: theft of trade secrets, theft or destruction of intellectual property, fraud, and other civil cases involving wrongful dismissals, breaches of contracts, and discrimination issues.

Recovered computer data often is a gold mine in a fraud investigation. Perpetrators may feel they have covered their tracks by deleting files, but computer forensics tools often allow nearly full recovery. Forensic examinations involve the examination of computer media, such as CD-ROMs, hard disk drives, backup tapes, and any other media used to store data. The forensic specialist uses specialized software to discover data that resides in a computer system or can recover deleted/erased, encrypted, or damaged file information and recover passwords, so that documents can be read.

Computer forensics is one approach to aid computer fraud investigations. This area requires specialized tools and training, and many internal auditors probably do not have the skills to perform such an analysis without obtaining help. As an indicator of interest in this area, the AICPA has just launched a new credential, Certified in Financial Forensics (CFF), that will combine specialized forensic accounting expertise with the core knowledge and skills that make CPAs trusted business advisors in this area. The CFF was announced as this book was being prepared; an internal auditor with a CPA background may want to investigate CFF credentials.

Other than direct testimony by an eyewitness, documentary evidence is usually the most compelling form of evidence, and paper trails traditionally have been a gold mine for IT fraud investigators. In past years, documentary evidence was limited to paper. Where the best evidence rule applied, the original document was produced. However, documents are rarely typed today; instead, they are produced on personal computer word processors. Some of these documents are e-mailed or faxed to the recipient directly from the computer. Because of the change in the way information is distributed and/or the way people communicate, copies of computer files are now as good as the original electronic document.

We have used computer forensics here as an example of a new technology-based technique for fraud detection. Firewall software to protect a system or user from entering transactions or accessing systems beyond a fixed region is another example. Virus protection software is a third. A full discussion of computer fraud aspects is beyond the scope of this book. The internal auditor must realize that computer fraud is a large and complex area.

25.7 Fraud Detection and the Internal Auditor

Fraud has always been with us, no matter how well we build strong standards for honesty, through codes of conduct and the like, and build ever stronger controls to prevent fraud. Badly burned by the accounting scandals that led to SOx, the AICPA and external auditors have taken on a major task to better detect fraudulent activities in their financial statement audits. Time will tell how effective the SAS No. 99 rules are, but the standard calls for a new dimension of thinking when planning and conducting financial statement audits.

Internal auditors need to give greater consideration to fraud in their audit work. When called on to do so by management, internal auditors often have been involved in some level of fraud investigation work, but today fraud detection and prevention considerations need to become a more significant component of every internal audit. Similar to the guidance in SAS No. 99, internal auditors perhaps need to enter new internal audit engagements by asking themselves some questions about how or where a new auditee might commit a fraudulent act. Internal auditors should always consider the potential for fraud in their ongoing work assignments.

Internal auditors should have a general CBOK level of understanding of the red flags that indicate a possibility of fraud as well as general internal audit review procedures that include an investigation for fraud in the course all internal audits. An internal auditor, however, should not begin a typical new internal audit with the expectation that the auditee is somehow fraudulent or dishonest. Rather, the internal auditor should understand that fraud can exist at many levels, and where there is a suspicion in the course of a review, the internal auditor should have the knowledge to report the matter to proper authorities and to assist in any fraud investigation as requested.

Notes

1. Ernst & Young, "Fraud, the Unmanaged Risk," 8th Global Survey, New York, 2003.
2. We have used the word *last* because the PCAOB took responsibility for issuing major external auditing standards shortly after the release of SAS No. 99.

3. Association of Certified Fraud Examiners, the Institute of Internal Auditors, and the American Institute of Certified Public Accountants, *Managing the Business Risk of Fraud: A Practical Guide,* exposure draft, issued November 12, 2007.
4. The federal fraud statute is referenced in a series of rules such as 18 U.S.C. 1341 on mail fraud and 18 U.S.C. 1344 on bank fraud.
5. ACEF, IIA, and AICPA, *Managing the Business Risk of Fraud*.
6. A *gigabyte* is a unit of information or computer storage meaning either exactly 1 billion bytes (1000^3, or 10^9) or approximately 1.07 billion bytes (1024^3, or 2^{30}). An internal auditor should think of a byte as a single character.

CHAPTER 26

HIPAA, GLBA, and Other Compliance Requirements

As discussed throughout this book, the Sarbanes-Oxley Act (SOx) has been the most significant U.S. accounting and securities legislation since the early 1930s. While SOx has launched a series of rules for corporate governance and financial statement auditing, other recent legislation has also introduced some new rules that have also impacted many enterprises and their internal auditors. This chapter introduces several of these newer U.S. federal acts that have improved internal controls and privacy protection focuses; this legislation with a U.S. focus impacts many modern enterprises and their internal auditors. Some of the compliance legislation requires a strong internal auditor common body of knowledge (CBOK) knowledge and understanding when the legislation impacts an internal auditor's industry, while others require an internal auditor CBOK level of awareness and general understanding.

This chapter looks at three items of legislation with wide impact, particularly for U.S.-based internal auditors. The first of these is the Health Insurance Portability and Accountability Act (HIPAA). An internal auditor might argue, "I do internal audits for a manufacturing company. Why should I worry about health insurance–related legislation?" HIPAA's focus is on healthcare providers, but it addresses a wide range of personal privacy records that impact all U.S. enterprises, and it has caused changes in such areas as information technology (IT) security and human resource (HR) functions. Every enterprise that carries employee health insurance data in its HR records needs to be aware of HIPAA rules, and internal auditors can often be a major aid to management in highlighting potential HIPAA controls and violation.

Popular descriptive titles for U.S. federal legislation often is based on the names of its original legislative sponsors. For example, Senator Paul Sarbanes and Representative Michael Oxley have brought us the Sarbanes-Oxley Act. Another legislative item of about the same period is the Gramm-Leach-Bliley Act of 1999 (GLBA) named after Senator Phillip Gramm and others. This legislation requires financial institutions to further protect and audit their data and to take special care when sharing these data with others. While directed at financial institutions, GLBA impacts many enterprises, and this chapter discusses its main components affecting internal auditors.

Going beyond SOx and GLBA rules discussed in this chapter and industry standards, such as the public key encryption data security standards rules (i.e., Payment Card Industry Data Security Standard [PCI-DSS]) discussed in Chapter 20, internal auditors worldwide encounter a wide range of often industry-specific compliance rules.

Many of these rules cover such areas as banking, securities, and electrical power generation. In other instances, U.S.- or E.U.-specific internal governance rules have implications that spread beyond just large governmental units. An example here is the U.S. Department of Commerce Office of Management and Budget (OMB) A-123 internal control guidelines, which often have very broad impacts on government agencies. The field is vast and comprehensive; this chapter summarizes some of the rules that may impact many internal auditors.

It is sometimes difficult to predict when newer legislation will have a continuing and lasting impact or whether it will be just a law on the books with little ongoing compliance impact activity. A U.S. example here is the Foreign Corrupt Practices Act (FCPA) of the late 1970s. That legislation had some strong internal control documentation requirements, and initially many internal auditors thought keeping their enterprises in compliance with FCPA provisions would keep them very busy. The legislation is still on the books, but there has been limited enforcement action since its enactment, and FCPA requirements covering internal control documentation have been all but forgotten. It is unlikely that GLBA, HIPAA, and SOx will go the same way as the FCPA, but the impact and enforcement actions for such legislation rise and fall. At the present time, internal auditors need to be aware of the privacy-related and compliance legislation discussed in this chapter and plan their review and internal control activities accordingly.

In particular, U.S.-based internal auditors should have a general CBOK understanding of GLBA and HIPAA rules. Although these two sets of rules focus primarily on consumer finance and healthcare issues that will not directly impact every internal auditor, both have important privacy provisions that are important in many other, broader areas. Of course, for an internal auditor working in a directly impacted industry, such as healthcare for HIPAA rules, a strong CBOK knowledge of the specific legislative rules is essential.

26.1 HIPAA: Healthcare and Much More

Although a healthcare-related set of rules, HIPAA contains a set of privacy-related legislative rules that go beyond healthcare and will impact many enterprises and their internal auditors. For example, a U.S.-based internal auditor who is visiting a doctor for an annual physical or some other procedure will be asked to sign a disclosure permission agreement when checking in. These permission documents ask patients to agree to allow their medical records to potentially be shared or disclosed as part of that visit. If the auditor-patient asks the reason for the document and why it must be signed, the response usually is that it is a "legal requirement of HIPAA." A patient typically signs the document and moves on, without asking further questions.

No matter where internal auditors work, they should have at least a general understanding of some HIPAA rules. Enacted in 1999 with the final rules released over subsequent years, HIPAA has had a major impact in the United States on the privacy and security of personal medical records and many others. As discussed, individuals encounter HIPAA when visiting a doctor's office or for many other medical-related matters. HR functions in enterprises are also seeing the impact of HIPAA requirements today in their administration of employee healthcare plans and medical records. Of course, HIPAA has had a large and growing impact on the entire healthcare industry and all affiliated delivery providers. Even more

significantly, HIPAA rules cover a wide range of business processes based on electronic commerce.

The original HIPAA legislation has four primary objectives:

1. **Ensure health portability by eliminating preexisting condition healthcare restrictions.** This was the original motivation that led to the passage of HIPAA. People who were diagnosed with some condition often were unable to acquire new health insurance coverage when changing employers because preexisting conditions were shared with potential new employers, who did not want to cover or insure those conditions.
2. **Reduce healthcare fraud and abuse.** The congressional hearings leading to the legislation cited examples of alleged fraud and abuse.
3. **Enforce standards for health information.** This enforcement is covered by the HIPAA privacy and security rules to be outlined in this chapter.
4. **Guarantee security and privacy of health information.** An overall objective of HIPAA is that healthcare information is a personal issue that should not be openly shared with others.

This section provides a brief overview of HIPAA objectives and its resultant rules covering privacy and security. The sections to come introduce HIPAA as a legislatively driven new set of rules that impact many internal auditors. The HIPAA legislation also illustrates how the government-sponsored rule-making process often works and hints at what we can expect from the new Public Company Accounting Oversight Board (PCAOB) auditing standards rules, beyond Auditing Standard No. 5 (discussed in Chapter 4). HIPAA rules were initially issued in draft form. The drafts resulted in many comments, revised drafts were issued with still more comments, and the final rules were issued much later than originally planned.

(a) HIPAA Patient Record Privacy Rules

Concerns regarding medical patient privacy were the motivating reasons for the U.S. Congress originally passing HIPAA. We visit a medical care provider, discuss some concern or problem, and then should expect confidential or private treatment regarding that medical visit. We do not want the results of the visit to be communicated to our employer's HR department or to some insurance company that has no need to know, or to be left on a desk in the medical provider's office for anyone to pick up. Even worse, we do not want any personal, confidential matters to be shared in a manner that may limit our future employment options. This personal information privacy concern is the basis for much of HIPAA. However, many parties need to have some information about our healthcare condition to provide adequate coverage or reimbursement, and virtually all healthcare operations require detailed and complex supporting systems. HIPAA privacy rules cover five general areas, which are briefly outlined next. These comments do not provide an exhaustive coverage of and are not intended to be a reference source for HIPAA rules; they are intended to provide the nonmedical professional with an overview of these HIPAA new rules:

1. **Medical records uses and disclosures** . An enterprise that is subject to HIPAA rules must take steps to limit the use and disclosure of personal medical information to "the minimum necessary to accomplish the intended purpose of

the use, disclosure, or request" for non–treatment-related matters. We start this overview of HIPAA rules by directly quoting some of the words contained in these rules. Using expressions such as "the minimum necessary," the act contains many such guidelines that will be subject to enterprise-specific practices that are to be validated through other rulings or litigation over time.

HIPAA rules specify that an individual's health information loses its HIPAA protection if the individual covered is "de-identified" in a manner that this health information will not contain any of 18 specific identifiers of the individual and relatives, employers, or household members. This requirement says a lot about HIPAA. In order to make a health-related information system HIPAA compliant, the legislation identifies these 18 specific factors that a specialist in database retrieval might use to identify an individual. That is, an individual's medical information that is placed in some type of file or information system is generally protected from general disclosure to others, but that information can be shared if it meets certain specific conditions.

2. **Authorization requirements.** This is the section of HIPAA that many users of healthcare services first encounter. Healthcare providers must obtain written approval to disclose healthcare information on everything except in emergency situations. An individual has the right to refuse such a disclosure, and healthcare providers must have a strong record retention requirement to keep track of all these disclosures. These are the documents, mentioned earlier, that individuals are asked to sign when visiting a physician's office.
3. **Privacy practice communications.** Healthcare providers must have published privacy practices that they should supply to healthcare users. Individuals then have the right to formally request restrictions in this policy, and providers must accommodate reasonable requests.
4. **Medical record access and amendment rights.** Individuals have the right to inspect and copy all or a portion of their personal health information. In addition, individuals have the right to request amendments to those healthcare records. Finally, the healthcare provider must keep a record of all other parties that requested access to an individual's personal healthcare records for a period of six months.
5. **HIPAA privacy administration.** Going beyond the records access and disclosure rules, HIPAA has an extensive set of privacy administrative requirements that apply to what are called "covered entities"—medical offices, laboratories, hospitals, and all others involved with personal healthcare. These privacy administration rules include:
   - The provider must designate a "Privacy Official" who is responsible for the development and implementation of these HIPAA policies and procedures.
   - The provider must train members of its workforce on these HIPAA privacy-related policies and procedures and must maintain documentation to demonstrate that the training has been provided.
   - A healthcare provider must have in place administrative, technical, and physical safeguards to protect the privacy of personal health information.
   - The healthcare provider must apply "appropriate sanctions" against employees who fail to comply with these privacy policies and procedures.
   - The provider must develop and implement policies and procedures that are designed to comply with the elements of the HIPAA regulations, and this documentation must be maintained in written or electronic form for six years.

While HIPAA rules primarily cover access to personal healthcare information, they also define good operating practices that should be implemented elsewhere in the enterprise. An example would be the requirement that healthcare providers maintain documentation covering their training programs. These types of rules have existed for Federal Drug Administration medical or drug programs, are now part of HIPAA, and are a good idea for most corporate training programs. Enterprises sometimes spend resources in training their employees but often do not bother to document that activity very well.

The HIPAA rules in this chapter are particularly important to an internal auditor working in a healthcare-related enterprise, such as a hospital or medical claims insurance company. However, the rules extend to other areas, such as medical insurance claims processing in an enterprise's HR department or factory floor safety and industrial accident reporting. Healthcare-related enterprises should have strong HIPAA compliance rules and procedures, but a detailed description of these rules is beyond the scope of this book. Internal auditors will encounter areas where HIPAA compliance is required in many other environments. Exhibit 26.1 describes some HIPAA healthcare procedures that should be in place in any enterprise

(b) Cryptography, PKI, and HIPAA Security Requirements

In addition to its medical records authorization and release privacy rules, HIPAA contains some very specific and, for smaller enterprises, difficult-to-implement IT security requirements. It pushes security practices to the edges of IT today and requires such things as secure electronic signatures, even though at this time there are limited technically mature techniques to provide such security on open networks such as the Internet. We are still at a point where a skilled computer hacker can intercept cell phone calls; such a call covering healthcare-related matters could create a violation of HIPAA security requirements. Technology will change in the future, control procedures will improve, the hackers will get ever smarter, and violations will be settled in the courts.

The basic reason behind these rules was that the security of many healthcare administrative systems in pre-HIPAA days was often inadequate. Enterprises can improve their security not by just purchasing and installing new software but by first improving human-driven policies. The HIPAA Security Standards rules were not finalized and put into effect until April 2003, and compliance for these rules did not take effect until 2006. Among other areas, these rules include what HIPAA calls "covered entities" such as:

- Doctors and other healthcare providers who process healthcare claims electronically
- Health plans, including enterprises that "self-insure"
- Healthcare clearinghouses—billing services and others that provide data formatting services for electronic claims submission

Thus, HIPAA security rules apply to all enterprises, whether a single doctor's office, a major hospital, or a small professional office that handles its own healthcare claims processing through self-insurance.

Security is a key element of keeping personal health information private, and HIPAA rules cover good security practices for much more than just medical records,

EXHIBIT 26.1 Internal Audit HIPAA Requirements Procedures

1. Is the enterprise defined as a healthcare-related enterprise and subject to HIPAA rules? (If not, no need to complete steps.)
2. Has an enterprise-wide information security officer been appointed for HIPAA compliance, and has a general implementation plan been developed?
3. Have policies and procedures to protect patient health information been developed and implemented?
4. Is there a process for the ongoing support and monitoring of HIPAA rules and regulations?
5. Are processes in place to develop comprehensive privacy and security policies, procedures, controls, and technologies?
6. Does the enterprise have a formal contingency plan in place that includes:
   - Application and data criticality analysis
   - Data backup planning
   - Disaster recovery plans
   - Emergency mode operations plan
   - Periodic testing and revisions to the plan
7. Are there formal information access control processes, including access authorization, access establishment rules, and access modification procedures?
8. Controls over access to information systems media should include processes for:
   - Accountability
   - Data backup
   - Data storage
   - Disposal of data
9. Personnel security policy/procedures should:
   - Ensure the supervision of maintenance personnel by an authorized, knowledgeable person
   - Maintain a complete record of access authorizations
   - Ensure that operating and maintenance personnel have proper access authorization
   - Establish a personnel clearance procedure
10. Formal termination procedures should be in place, including the changing of appropriate combination locks and the removal from access lists.
11. Physical access controls throughout the facility should include:
    - Emergency mode operation plans
    - Equipment control into and out of the facility
    - Facility security plans
    - Procedures for verifying access authorizations prior to physical access
    - Maintenance records
    - Need-to-know procedures for personnel access
    - Sign-in for visitors and escort, if appropriate
    - Testing and revisions to the physical access plan
12. All networks and communications should be protected through:
    - Automatic log-off
    - Unique user identification
    - Passwords and personal identification numbers.
    - Telephone callbacks.

such as requirements for strong disaster recovery standards. The published rules consist of both "required" and what HIPAA calls "addressable" rules. The latter are rules that an enterprise is not required to implement due its small size and limited resources. The "required" HIPAA rules represent many good information security practices that are appropriate to any enterprise. Other HIPAA security areas here are

beyond the scope of this book, such as requirements for a Public Key Infrastructure (PKI) environment that includes digital signatures.

(c) HIPAA Security Administrative Procedures

HIPAA requires administrative procedures to be in place to guard data integrity, confidentiality, and availability. These procedures must be carefully documented per HIPAA rules, and Exhibit 26.2 lists some of these "required" administrative procedures. The exhibit also lists the implementation rules in a very general manner; published HIPAA rules tend to be very detailed. Many of these requirements, such as a requirement for a documented and tested contingency plan or formal policies for information access controls, are similar to the control procedures internal auditors have been recommending over the years. Others represent good practices that

EXHIBIT 26.2 HIPAA Required Implementation Specifications

These provisions apply to what are called "covered" entities or enterprises under HIPAA rules and must be part of an enterprise's HIPAA security and compliance plan.

1. **Risk analysis.** Enterprises must conduct a thorough assessment of the potential risks of information confidentiality, integrity, and availability.
2. **Risk management.** Covered enterprises must implement reasonable and appropriate security measures to reduce overall risks to an acceptable level.
3. **Sanctions policy.** Sanctions or related penalties must be applied to workforce members who violate the enterprise's security policy. This might translate into some type of a three-strikes-and-you're-out policy.
4. **Information systems security activity reporting.** Security logs, incident reports, and related security activity reports should be reported and reviewed on a regular basis.
5. **Incident response.** Processes should be in place to identify, investigate, mitigate, and document security incidents.
6. **Backup procedures.** Appropriate procedures must be in place to recover any loss of data.
7. **Disaster recovery.** Every covered enterprise must establish procedures to cover any loss of data.
8. **Emergency mode of operations.** Processes must be in place to ensure the security of patient information when operating in an emergency mode.
9. **Related business contracts.** An enterprise must include language in contracts with suppliers of related services that require the supplier to adopt adequate security measures to report security incidents to the enterprise, to ensure these subcontractors implement appropriate security measures, and to provide for the termination of the contract in case of a security breach.
10. **Disposal of patient information.** Policies and procedures should be in place to address the final disposition of such patient information as recycled disc devices.
11. **Media reuse.** Processes must be in place to ensure the removal of sensitive information from electronic media, such as disc drives, before reuse.
12. **Unique user identification** Unique identifiers must be assigned to all systems users in order to prevent shared accounts and to track system behavior.
13. **Emergency access procedures.** Procedures must be established to allow for the accessing of electronic information during an emergency.
14. **Documentation.** Procedures must be established to guarantee information security, maintain the documentation for a period of six years, and review it periodically.

should be in place in many enterprises. Rule 3 in the exhibit refers to the need for what is called a sanctions policy—a formal set of rules for people who violate security policy. This is a good idea for most enterprises. Today, as an administrative rule, a U.S.-based HIPAA-impacted healthcare provider will face a penalty if its established rules and procedures are found inadequate.

HIPAA security requirements also include some physical safeguard rules that are similar to the physical access controls that have existed for years over IT data centers. Here, however, HIPAA goes beyond the classic IT operations center and calls for strong guidelines and documentation over workstation use and location. While internal auditors typically have not raised that many internal control concerns regarding the physical controls for networked terminals in a business environment, the HIPAA-regulated healthcare environment introduces new issues. A medical environment workstation that is used by doctors, nurses, and/or other staff members requires strong logical and physical controls to protect the personal privacy of the patient records that pass through those workstations.

(d) Technical Security Services and Mechanisms

HIPAA rules require that processes should be put in place to guard the integrity, confidentiality, and availability of these medical records data and to prevent unauthorized access to any data that are transmitted over communications networks. The rules here require information systems security controls that are often stronger than those found in some larger corporations today and include:

- **Access control.** Strong control mechanisms based on the context of the data or the role/position of authorized users must be established. In addition, control processes must always be in place to allow emergency access from data center operations if required.
- **Audit controls.** Here and throughout all of the HIPAA rules are requirements for strong audit controls, including such things as documentation revision processes and traditional audit trails.
- **Data authentication.** Strong systems controls over data integrity are required. These are the same types of application controls discussed in Chapter 19.
- **Entity authentication.** Controls must be in place such that when one workstation attempts to access another, it should be authenticated. This process may include passwords, telephone callbacks, or even biometric controls. This requirement goes beyond many enterprise practices in place today where information is often freely shared through an e-mail note with attachments.
- **Communications and network controls.** A wide range of controls are suggested here, including alarms, encryption, event reporting, message authentication, and others. The HIPAA-impacted enterprise must implement a very secure network.

HIPAA requires that electronic signature controls be established that will provide the same legal weight to electronic data signatures as is associated with a traditional signature on a paper document. HIPAA prescribes network message integrity, no repudiation, and user authentication for any message with an electronic signature. For many organizations, this can be a challenge. Digital signature processes in place today often are somewhat cumbersome but will be required until other, better techniques are developed. This is a classic case of the U.S. government establishing ideal

or desired rules even when no practical solution exists today. Legislators sometimes think that if they set a high standard, industry and other groups will charge ahead to make things happen. This sometimes does work, but if not, rules will need to be revised.

(e) Going Forward: HIPAA and E-Commerce

Although designed to protect and authenticate medical information, HIPAA rules outline some strong guidelines for all electronic commerce processes. A major requirement here will be improved standards and processes for electronic signatures. More needs to be accomplished before processes become common and commercially available, and the National Institute of Standards and Technology (NIST) is taking a leadership role in the development of a Federal Public Key Infrastructure that supports digital signatures and other public key–enabled security services. NIST today is coordinating with industry and technical groups developing PKI technology to foster interoperability of PKI products and projects. There should be more changes going forward,

HIPAA rules have pushed progress in many areas of IT security and integrity. Although developed for healthcare enterprises, these rules impact many enterprises. Internal auditors should try to stay aware of these rules and required standards even if they do not work directly for a healthcare enterprise. Beyond just pertaining to healthcare enterprises, these complex and important rules apply whenever health-related records are maintained by a HR function. An internal auditor can find more HIPAA information on the Web from two important sources:

1. **U.S. Department of Health and Human Services.** Copies of HIPAA rules and other supporting reference materials are available from http://hhs.gov/ocr/hipaa.
2. **HIPPA Advisories.** A site maintained by Phoenix Health Systems as a public service is a good source for HIPAA information; see www.hipaadvisory.com.

HIPAA compliance is a U.S. legal requirement. While government auditors are not going to be visiting hospitals, large healthcare facilities, or HR departments of commercial organizations, an individual who feels there has been a violation can file a complaint with the U.S. Department of Justice (DOJ). That could certainly occur if some key information from an employee's medical insurance claim records became public knowledge due to a records security breakdown. The DOJ has a complaint-driven/voluntary compliance approach.

If the DOJ decides to take action regarding some complaint, it currently has a one-free-violation policy. In other words, first the DOJ will work with the noncomplaint organization; if corrective action is not attained, the DOJ will consider the imposition of civil monetary penalties.

Internal auditors should be aware of HIPAA rules, at least on a high level. Internal auditors should recommend strong security and confidentiality controls over any area that might impact an employee's medical health records.

26.2 Gramm-Leach-Bliley Act Internal Audit Rules

Officially known as the Financial Modernization Act of 1999, the GLBA is a privacy-related set of U.S. requirements with an objective to protect consumers' personal

financial information that is held by financial institutions. This legislation has three principal parts:

1. The Financial Privacy Rule
2. The Safeguards Rule
3. What is called its "pretexting provisions"

GLBA gives authority to eight different U.S. federal agencies and the states to administer, and it enforces a new set of privacy-release rules that apply to what are generally called "financial institutions." These institutions include not only traditional banks, securities firms, and insurance companies, but also enterprises providing many other types of financial products and services to consumers. Among these are the lending, brokering, and servicing of any type of consumer loans, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, residential real estate settlement services, collecting consumer debts, and an array of other activities. With GLBA, these nontraditional "financial institutions" are now regulated by the Federal Trade Commission (FTC) either directly or through other federal and state agencies.

Internal auditors working for banks or insurance companies probably have been impacted by GLBA and its privacy-related provisions. The act also may cover many other enterprises due to its expanded definition of what are called "financial institutions." For example, GLBA rules also apply to many state-regulated financial institutions. Insurance companies in the United States are regulated on a state-by-state basis with the National Association of Insurance Commissioners (NAIC) acting as a central coordinating and standards-setting group. The NAIC has imposed the federally mandated GLBA rules on its individual state-regulated insurance companies. This is another example of how U.S. federal regulations sometimes move from a U.S. authority to rules covering state laws as well as some similar international rules. Although the certified public accountant (CPA) examination is administered by the American Institute of CPAs (AICPA), CPAs are licensed on an individual state basis through individual boards of accountancy. Through the authority of the NAIC, a state rule coordinating body, GLBA rules are being adopted by most to the states in the United States.

(a) GLBA Financial Privacy Rules

U.S. consumers frequently encounter the GLBA and its Financial Privacy Rule today when they receive a note from a credit card provider talking about privacy rules for that credit card. The GLBA Financial Privacy Rule requires financial institutions to give customers these privacy notices that explain the financial institution's information collection and sharing practices. This privacy notice must be a clear, conspicuous, and accurate statement of an enterprise's privacy practices; it should include what information the enterprise collects about its consumers and customers, with whom it shares this consumer credit information, and how it protects or safeguards the information. The notice applies to the "nonpublic personal information" the enterprise gathers and discloses about its consumers and customers; in practice, that may be most—or all—of the information an enterprise has about its customers. For example, nonpublic personal information could include the information that a consumer or customer puts on a credit or sales contract application; information

about the individual from another source, such as a credit bureau; or information about transactions between the individual and the company, such as an account balance. Indeed, even the fact that an individual is listed as a consumer or customer of a particular financial institution is classified under GLBA as nonpublic personal information. Matters that the company has reason to believe are lawfully public—such as mortgage loan information in a jurisdiction where that information is publicly recorded—is not restricted by GLBA.

GLBA-mandated privacy notices must contain these information elements:

- The types of nonpublic personal information an enterprise collects regarding its customer
- The types of nonpublic personal information the enterprise will disclose to others about the customer
- The parties to whom the enterprise discloses this information, other than under an exception to the prohibition on nondisclosure
- The customer or client's right to "opt out" of the disclosure along with simple rules for opting out
- Enterprise policies with respect to sharing information about a person who is no longer a customer or client
- Enterprise practices for protecting the confidentiality and security the customer or clients' nonpublic personal information

Many consumers today pay little attention to these notices, even though they may state that the enterprise that has their account data may share the consumer's name with others. GLBA gives the customer the right to opt out of—or say no to—having this consumer private information shared with certain third parties. The privacy notice must explain how—and offer a reasonable way—they can opt out. For example, providing a toll-free telephone number or a detachable form with a preprinted address is a reasonable way for consumers or customers to opt out; requiring someone to write a letter as the only way to opt out is not. The privacy notice must also explain that consumers have a right to say no to the sharing of certain information, such as credit report or application information, with the financial institution's separate divisions or affiliates.

GLBA puts limits on how anyone who receives nonpublic personal information from a financial institution can use or redisclose that information. If a lender discloses customer information to a service provider responsible for mailing account statements, where the consumer has no right to opt out, that service provider may use the information only for limited purposes—such as for mailing account statements—and may not sell the information or use it for marketing.

The details of this GLBA Federal Privacy Rule are complex. Our intention here, however, is to explain these privacy rules in general. An internal auditor should recognize that all personal financial information is very private and cannot be just arbitrarily sold or otherwise distributed. Consumers have rights to opt out and say no, and the enterprise must keep appropriate records of these actions and respect consumer privacy rights. Internal auditors working with any financial institutions or applications, or for any enterprise that has a consumer-related credit granting and billing facility, should be aware of how GLBA privacy applies to the enterprise. Enterprises that consider the GLBA Privacy Rules as a trivial matter and perhaps fail

to honor an opt-out request or improperly sell a mailing list, may find themselves facing class action litigation for damages due to the failure to comply.

(b) GLBA Safeguards Rule

The act's Safeguards Rule requires financial institutions to have a security plan in place to protect the confidentiality and integrity of personal consumer information. When consumers open an account or purchase a product, they often disclose some element of their personal information—an address, telephone number, or credit card number—as part of that application transaction process. An enterprise must have a security plan in place to protect the confidentiality and integrity of that consumer-supplied personal data. The plan should cover more than just the business continuity risks discussed in Chapter 22 and include controls to prevent hackers from accessing data files, disgruntled employees accessing customer information, or simple carelessness. The GLBA Safeguards Rule requires that every financial institution, regardless of size, must create and implement a written information security plan for the protection of customer data. The scope and complexity of this security plan may be scaled to the size of the institution and the sensitivity of the information it maintains. The plan should be based on a risk analysis that identifies all foreseeable threats to the security, confidentiality, and integrity of customer information. Based on that risk analysis, financial institutions must document and implement security measures that include administrative measures such as employee training; technical protections including passwords, encryption controls, and firewalls; and physical safeguards such as locks on doors and computers. Financial institutions must designate one or more of their employees to coordinate these safeguards and must conduct periodic reviews to determine whether their security programs require updating in light of changed circumstances.

Internal auditors should be aware of how a U.S.-based enterprise can demonstrate compliance with the GLBA safeguard rule through five steps:

1. **Environmental risk analysis.** The enterprise should formally identify the internal and external risks to the security, confidentiality, and integrity of all customer personal information. Risk analysis approaches were discussed in Chapter 6. This process should cover the risks of loss or disclosure for all sources of personal information, whether on automated systems or manual records.
2. **Designing and implementing safeguards.** These safeguards are essentially the internal control procedures discussed in Chapter 3 as part of the Committee of Sponsoring Organizations (COSO) internal controls framework and elsewhere throughout this book.
3. **Monitoring and auditing.** Continuous audit assurance monitoring processes, such as discussed in Chapter 29, should be in place. Internal audit can play an important monitoring and auditing role here by regularly scheduling reviews of the adequacy of the security plan, coupled with appropriate compliance tests.
4. **Constant improvements program.** The enterprise should have a program in place to constantly improve its security plan. That program should be well documented to describe the plan's progress in improving any weaknesses found.
5. **Overseeing security providers and partners.** Many partners and other enterprises may have access to this same personal information or to systems network connections where personal privacy can be violated. Adequate policies, controls, and audit procedures need to be in place here as well.

The GLBA Safeguards Rule applies to a wide range of providers of financial products and services, including mortgage brokers, nonblank lenders, appraisers, credit reporting agencies, professional tax preparers, and retailers that issue their own credit cards. Banks are not subject to the Safeguards Rule but must comply with similar counterpart regulations that have been issued by federal banking agencies. Failure to comply with the Safeguards Rule may result in fines or other enforcement action by the FTC.

(c) GLBA Pretexting Provisions

GLBA prohibits "pretexting"—the use of false pretenses, including fraudulent statements and impersonation—to obtain consumers' personal financial information, such as bank balances, under false pretenses. Pretexters use a variety of tactics to get personal information. For example, a pretexter may call, claim to be from a survey firm, ask a few questions to perhaps get the name of one's bank, and then use the information gathered to call the target person's financial institution, pretending to be that targeted person or someone with authorized access to that account. The caller might claim to have forgotten her checkbook and needs information about the account. In this way, the pretexter may be able to obtain personal information about the target victim, such as a Social Security number, bank and credit card account numbers, information in a credit report, and the existence and size of personal savings and investment portfolios.

Under GLBA's Pretexting Provisions, it is illegal for anyone to:

- Use false, fictitious, or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Use forged, counterfeit, lost, or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Ask another person to get someone else's customer information using false, fictitious, or fraudulent statements or using false, fictitious, or fraudulent documents or forged, counterfeit, lost, or stolen documents.

Pretexting leads to a new security and privacy risk or exposure: identity theft. This occurs when someone hijacks your personal identifying information to open new charge accounts, order merchandise, or borrow money. Consumers targeted by identity thieves usually do not know they have been victimized until the hijackers fail to pay the bills or repay the loans, and collection agencies begin dunning targeted consumers for payment of accounts they did not even know they had. According to the FTC, the most common forms of identity theft are:

- **Credit card fraud.** A credit card account is opened in a consumer's name or an existing credit card account is "taken over."
- **Communications services fraud.** The identity thief opens telephone, cellular, or other utility service in the consumer's name.
- **Bank fraud.** The identity thief opens a checking or savings account in the consumer's name and/or writes fraudulent checks.
- **Fraudulent loans.** The identity thief gets a loan, such as a car loan, in the consumer's name.

A separate U.S. law related to GLBA is the Identity Theft and Assumption Deterrence Act, which makes it a federal crime when someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law." Here, a name or Social Security Number is considered a "means of identification," as is a credit card number, cellular telephone electronic serial number, or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual.

GLBA is a rule that can impact many internal auditors, particularly those working in any type of financial institution. While many aspects of GLBA are designed primarily to protect consumer financial information, its definitions are so broad that GLBA potentially impacts a wide range of enterprises and many U.S internal auditors.

Internal auditors working with financial and credit-granting enterprises should become more aware of these GLBA rules as well as the general privacy rules that are applicable for many other enterprises. The Web is a good source to obtain additional more detailed and current information on the act and its provisions. Two good sources are:

1. **Federal Trade Commission.** This government source provides an overview view of GLBA as well as its most current rules at: www.ftc.gov/privacy/glbact.
2. **National Association of Insurance Commissioners.** This is the state-by-state regulatory enterprise that has good GLBA information at: www.naic.org/GLBA.

Exhibit 26.3 provides some general rules and steps for auditing compliance with GLBA controls and procedures. While these audit procedures must be expanded for some enterprises, the objective of this exhibit is to provide some general audit steps to consider for an internal audit operational review of financial institutions to demonstrate GLBA compliance.

26.3 Other Personal Privacy and Security Legislative Requirements

GLBA and HIPAA are two important privacy and security legislative initiatives that should remain on U.S.-based internal auditors' radar screens. These are in addition to the due care standards of the PCI-DSS discussed in Chapter 20. There are also other recent privacy-related U.S. federal initiatives, such as the Children's Online Privacy Protection Act (COPPA), which regulates the collection of children's personal information. In addition, some 35 (and counting) U.S. states have introduced their own data protection acts. Because these rules are not always consistent from state to state, compliance can become a major challenge. An enterprise's legal counsel is the authority most aware of these issues, and internal audit should coordinate activities closely with its legal counsel to ensure that internal audit reviews recognize and support these legal compliance rules.

Other related regulatory drivers exist on a worldwide basis and include the European Union Data Protection standard, the Canadian Personal Information Protection and Electronic Documents Act, and a Japanese Data Protection law. Each of these has data security requirements that are common to HIPAA data security rules. Another international privacy and security standard is the International Standards

EXHIBIT 26.3 Internal Audit Procedures for Gramm-Leach-Bliley Compliance

Internal audit should meet with financial management and corporate counsel to assess whether the enterprise can be defined as a "financial institution" under the terms of the Gramm-Leach-Bliley Act (GLBA). If impacted, internal audit procedures should:

1. Determine the enterprise regularly sends out financial privacy notices, and assess follow-up procedures in place to correct returned letters or to provide answers to customers regarding these notices.
2. Assess record-keeping and other controls regarding the privacy notice opt-out rules. Select a sample of customers who have requested to opt out and determine that these privacy procedures are operating.
3. Review general record privacy and security procedures over all GLBA-impacted materials. Good practices here include strong information systems password controls and office procedures covering paper-oriented records.
4. Determine that the enterprise has a formal security plan in place to protect the security and confidentiality of personal consumer information.
5. Determine that an environmental risk analysis is in place to formally identify all internal and external risks to the security, confidentiality, integrity of all customer personal information.
6. Review continuous monitoring processes in place surrounding controls over customer personal information, and assess their adequacy.
7. Review the adequacy of constant improvements programs surrounding GLBA security controls, and comment on their adequacy.
8. Assess the adequacy of information programs within the enterprise to inform all employees on the requirements of GLBA and their need to protect customer personal information.
9. Determine that adequate controls are in place to prevent violations of GLBA pretexting provisions.
10. Determine that the enterprise has taken adequate steps to inform other related organizations of GLBA provisions.

Organization (ISO) no. 15408, a framework to evaluate IT security. ISO standards are introduced briefly in Chapter 30. A common thread for these initiatives is the personal privacy protection for information about an individual kept in IT systems records.

The HIPAA and GLBA legislation discussed in this chapter may very well point to other legislative initiatives in areas beyond healthcare and personal financial privacy protections. In addition, although it may take some time to develop fully, the COSO enterprise risk management risk model discussed in Chapter 6 may soon cause some major changes in how we understand, organize, and protect business and other risks. There will be many opportunities for internal auditors in current and future organizations. Internal auditors, at all levels, should have a high-level CBOK awareness of these rules. When an internal auditor is working in a healthcare or financial enterprise that is directly impacted by HIPAA or GLBA rules, a strong CBOK understanding of these rules and how they impact internal audit activities is essential.

PART VII

The Professional Internal Auditor

CHAPTER 27

Professional Certifications: CIA, CISA, and More

We live in world today increasingly filled with various and sometimes too many professional certification designations. For example, a civil engineer designing highway bridges will seek a very important and well-recognized professional engineer (PE) certification; a household interior designer may take examinations to become a certified kitchen designer (CKD). These certifications may be viewed very positively by an employer or customer looking for a candidate to fill a position requiring appropriate job skills. A CKD may give a candidate some additional points in the job selection process.

Many professional certifications are viewed as worthwhile, but others do not seem that valuable. For example, and not to pick on an industry, the insurance industry is filled with many types and levels of certifications. A potential purchaser of life insurance, for example, may encounter a salesperson with a stream of certification initials after the name on the business card. Does such a Certified Life Underwriter (CLU) credential have an influence on whether a consumer will buy life insurance from one salesperson over another? For many, the answer is probably no. Those initials may help tell the consumer that the life insurance salesperson is experienced, but often the sales pitch and price are deciding factors on the insurance purchase. Of course, the consumer will expect a greater knowledge of insurance processes from the salesperson with the CLU.

Internal auditors also have a need for strong and well-recognized professional certification. Many have joined the profession with no specific certification requirements beyond their undergraduate college degrees. Others attained accounting degrees and prepared for the Certified Public Accountant (CPA) examination. Once hiring managers assumed that potential internal auditor candidates must have a CPA to become qualified as an internal auditor, but over time many realized that the internal audit profession requires people with more qualifications than just a CPA. Things changed at the urging of Institute of Internal Auditors (IIA) professionals, and the result was the Certified Internal Auditor (CIA) certification. Today, beyond or separate from the CIA, an internal auditor can become a Certified information Systems Auditor (CISA), a Certified Fraud Examiner (CFE), or any of a series of other certifications. Some of these may be very valuable for typical internal auditors; others may not be. This chapter discusses the professional designations that are most important to the modern internal auditor. In particular, this chapter looks at the CIA and CISA certifications, including their qualification and examination requirements.

The chapter also considers some other certification options available to internal auditors.

The chapter does not discuss the CPA examination. While certainly more oriented to external auditors, the CPA is still the best and most recognized accounting, auditing, and internal control examination for all financial professionals, including internal auditors. It should be an objective for any internal auditor with a financial background. The other professional examinations discussed in this chapter, such as the CIA, also should be considered a strong objective for many modern internal auditors.

27.1 Certified Internal Auditor Responsibilities and Requirements

Sponsored by the IIA, the CIA® designation is the only globally accepted certification for internal auditors and is the major standard by which individuals can demonstrate their competency and professionalism in internal auditing. The CIA examination was first offered in August 1974 to 654 candidates, and there are about 50,000 CIAs to date. Administered by the IIA Board of Regents, the CIA is an 11-hour examination offered worldwide through computer-based testing services. It consists of four parts:

Part I. The Internal Audit Activity's Role in Governance, Risk, and Control
Part II. Conducting the Internal Audit Engagement
Part III. Business Analysis and Information Technology
Part IV. Business Management Skills

By applying to become a CIA candidate, an individual agrees to accept the conditions of the program including eligibility requirements, exam confidentiality, acceptance of the CIA's code of ethics, continuing professional education (CPE), and any other conditions enacted by the Board of Regents or its Certification Department.

To apply to take the CIA examination, candidates must hold a bachelor's degree or its equivalent, such as Chartered Accountant, from an accredited college-level institution. A copy of the candidate's diploma, transcripts, or other written proof of completion of a degree program must accompany the candidate's application. With the exception of full-time undergraduate-degree students in their senior year, candidates will not be allowed to sit for the exam until the educational requirement is met.

Applicants who do not possess a bachelor's degree and who are unsure whether their educational achievements or professional designations qualify as equivalents can apply for a waiver from these educational requirements through a formal request to the Board of Regents, the final judge of the acceptability of professional or educational attainment offered in lieu of a bachelor's degree and of equivalents. Information submitted should be sufficiently detailed to enable the Board of Regents to determine equivalency.

CIA candidates must exhibit high moral and professional character and must submit a character reference completed by another CIA, the candidate's supervisor or manager, or an appropriate educator. In addition, CIA candidates are required to have completed 24 months of internal auditing or equivalent experience in audit/assessment disciplines, external auditing, quality assurance, compliance, or internal control–related work. Either a master's degree or work experience in related business professions (such as accounting, law, or finance) can be substituted for one year of experience. Work experience must be verified by a CIA or the candidate's

supervisor. Candidates may sit for the CIA exam prior to satisfying their experience requirement, but they will not be certified until the experience requirement has been met.

Candidates with other appropriate professional certifications can apply for a Part IV waiver. For example, in the United States, candidates with a CISA (discussed later in this chapter) or a CPA do not have to take Part IV. There are similar approved other professional certifications in countries around the world, such as a Chartered Accountant (CA) in the United Kingdom or Canada.

The CIA exam is "nondisclosed"; and candidates must agree to keep the exam contents confidential and should not discuss the specific exam content with anyone except the IIA's Certification Department. Unauthorized disclosure of exam material will be considered a breach of the code of ethics and could result in disqualification of the candidate or other appropriate censure.

(a) The CIA Examination

Exhibit 27.1 contains an overview of the potential contents of the CIA examination's four parts. These are general topic areas and may change over time. As shown on the exhibit, candidates may be tested for their proficiency (P) or awareness (A) in any given subject area. *Awareness* means that the candidate must have a general knowledge of the issues in a topic area; *proficiency* says the candidate should have a strong understanding and knowledge of how to apply that subject area. Two subject points from Exhibit 27.1 might better explain these differences:

- Section A on Business Processes from Part III on Business Analysis and Information Technology contains 10 subject areas, some labeled A and others P. Subject area 4 calls for the CIA candidate to have a proficient knowledge of project management techniques. This is certainly a common body of knowledge (CBOK) requirement, as outlined in Chapter 14.
- Section B on Financial Accounting and Finance in Part III on Business Analysis and Information Technology also has 10 subject areas, some labeled A and others P. Subject area 7 calls for the CIA candidate to have an awareness of financial instruments such as derivatives. In other words, a typical CIA internal auditor needs to have just a general understanding of financial derivative concepts.

The CIA examination covers a wide range of topics that are significant to the modern internal auditor. Each of the four sections has multiple choice examination questions. Each of the A or P topic areas in Exhibit 27.1 may or may not be covered in any particular examination. The exam is updated periodically and reflects current topics of interest to internal auditors. The internal auditor CBOK requirements outlined throughout this book are very close to Exhibit 27.1's internal auditor A and P CIA requirements. Virtually all of the CIA requirement topics outlined in the exhibit are outlined in chapters of this book. Our internal auditor CBOK differs with the IIA Board of Regents in a few areas. For example, in Part III, section B, point 4 calls for the CIA candidate to be proficient in financial statement analysis. Beyond a proficiency in simple financial ratio analysis, this CIA knowledge requirement may be asking internal auditor candidates too much. Conversely, section E of Part III only calls for internal auditors to be aware of the *C*ontrol *ob*jectives for *i*nformation and related *T*echnology (CobiT) framework. As discussed in Chapter 5, an

This exhibit outlines the concentration requirements for the Certified Internal Auditor (CIA) examination. Knowledge requirements are labeled P or A where:

P = Candidates must exhibit proficiency (thorough understanding and ability to apply concepts) in these topic areas.
A = Candidates must exhibit awareness (knowledge of terminology and fundamentals) in these topic areas.

Part I: The Internal Audit Activity's Role in Governance, Risk, and Control—*100 multiple-choice questions—2 hours and 45 minutes*

A. COMPLY WITH THE IIA'S ATTRIBUTE STANDARDS (15–25%)	LEVEL P
1. Define purpose, authority, and responsibility of the internal audit activity. a. Determine if the purpose, authority, and responsibility of internal audit activity are clearly documented and approved. b. Determine if the purpose, authority, and responsibility of internal audit activity are communicated to the engagement clients. c. Demonstrate an understanding of the purpose, authority, and responsibility of the internal audit activity. 2. Maintain independence and objectivity. 3. a. Foster independence. 1) Understand organizational independence. 2) Recognize the importance of organizational independence. 3) Determine if the internal audit activity is properly aligned to achieve organizational independence. b. Foster objectivity. 1) Establish policies to promote objectivity. 2) Assess individual objectivity. 3) Maintain individual objectivity. 4) Recognize and mitigate impairments to independence and objectivity. 4. Determine if the required knowledge, skills, and competencies are available. a. Understand the knowledge, skills, and competencies that an internal auditor needs to possess. b. Identify the knowledge, skills, and competencies required to fulfill the responsibilities of the internal audit activity. 5. Develop and/or procure necessary knowledge, skills, and competencies collectively required by internal audit activity. 6. Exercise due professional care. 7. Promote continuing professional development. a. Develop and implement a plan for continuing professional development for internal audit staff. b. Enhance individual competency through continuing professional development. 8. Promote quality assurance and improvement of the internal audit activity. a. Establish and maintain a quality assurance and improvement program. b. Monitor the effectiveness of the quality assurance and improvement program. c. Report the results of the quality assurance and improvement program to the board or other governing body. d. Conduct quality assurance procedures and recommend improvements to the performance of the internal audit activity. 9. Abide by and promote compliance with The IIA Code of Ethics.	
B. ESTABLISH A RISK-BASED PLAN TO DETERMINE THE PRIORITIES OF THE INTERNAL AUDIT ACTIVITY (15–25%)	**LEVEL P**
1. Establish a framework for assessing risk. 2. Use the framework to: a. Identify sources of potential engagements (e.g., audit universe, management request, regulatory mandate) b. Assess organization-wide risk c. Solicit potential engagement topics from various sources d. Collect and analyze data on proposed engagements e. Rank and validate risk priorities	

EXHIBIT 27.1 CIA Examination Summary

Source: Printed with permission of The Institute of Internal Auditors, 247 Maitland Avenue, Altamonte Springs, FL 32701-4201.

3. Identify internal audit resource requirements. 4. Coordinate the internal audit activity's efforts with: a. External auditor b. Regulatory oversight bodies c. Other internal assurance functions (e.g., health and safety department) 5. Select engagements. a. Participate in the engagement selection process. b. Select engagements. c. Communicate and obtain approval of the engagement plan from board.	
C. UNDERSTAND THE INTERNAL AUDIT ACTIVITY'S ROLE IN ORGANIZATIONAL GOVERNANCE (10–20%)	**LEVEL P**
1. Obtain board's approval of audit charter. 2. Communicate plan of engagements. 3. Report significant audit issues. 4. Communicate key performance indicators to board on a regular basis. 5. Discuss areas of significant risk. 6. Support board in enterprise-wide risk assessment. 7. Review positioning of the internal audit function within the risk management framework within the organization. 8. Monitor compliance with the corporate code of conduct/business practices. 9. Report on the effectiveness of the control framework. 10. Assist board in assessing the independence of the external auditor. 11. Assess ethical climate of the board. 12. Assess ethical climate of the organization. 13. Assess compliance with policies in specific areas (e.g., derivatives). 14. Assess organization's reporting mechanism to the board. 15. Conduct follow-up and report on management response to regulatory body reviews. 16. Conduct follow-up and report on management response to external audit. 17. Assess the adequacy of the performance measurement system, achievement of corporate objective. 18. Support a culture of fraud awareness and encourage the reporting of improprieties.	
D. PERFORM OTHER INTERNAL AUDIT ROLES AND RESPONSIBILITIES (0–10%)	**LEVEL P**
1. Ethics/Compliance a. Investigate and recommend resolution for ethics/compliance complaints. b. Determine disposition of ethics violations. c. Foster healthy ethical climate. d. Maintain and administer business conduct policy (e.g., conflict of interest). e. Report on compliance. 2. Risk Management a. Develop and implement an organization-wide risk and control framework. b. Coordinate enterprise-wide risk assessment. c. Report corporate risk assessment to board. d. Review business continuity planning process. 3. Privacy a. Determine privacy vulnerabilities. b. Report on compliance. 4. Information or physical security a. Determine security vulnerabilities. b. Determine disposition of security violations. c. Report on compliance.	
E. GOVERNANCE, RISK, AND CONTROL KNOWLEDGE ELEMENTS (15–25%)	**LEVELS**
1. Corporate governance principles 2. Alternative control frameworks	A A

EXHIBIT 27.1 CIA Examination Summary (*Continued*)

3. Risk vocabulary and concepts	P
4. Risk management techniques	P
5. Risk/control implications of different organizational structures	P
6. Risk/control implications of different leadership styles	A
7. Change management	A
8. Conflict management	A
9. Management control techniques	P
10. Types of control (preventive, detective, input, output)	P

F. PLAN ENGAGEMENTS (15–25%)	LEVEL P
1. Initiate preliminary communication with engagement client. 2. Conduct a preliminary survey of the area of engagement. a. Obtain input from engagement client. b. Perform analytical reviews. c. Perform benchmarking. d. Conduct interviews. e. Review prior audit reports and other relevant documentation. f. Map processes. g. Develop checklists. 3. Complete a detailed risk assessment of the area (prioritize or evaluate risk/control factors). 4. Coordinate audit engagement efforts with a. External auditor b. Regulatory oversight bodies 5. Establish/refine engagement objectives and identify/finalize the scope of engagement. 6. Identify or develop criteria for assurance engagements (criteria against which to audit). 7. Consider the potential for fraud when planning an engagement. a. Be knowledgeable of the risk factors and red flags of fraud. b. Identify common types of fraud associated with the engagement area. c. Determine if risk of fraud requires special consideration when conducting an engagement. 8. Determine engagement procedures. 9. Determine the level of staff and resources needed for the engagement. 10. Establish adequate planning and supervision of the engagement. 11. Prepare engagement work program.	

Part II: Conducting the Internal Audit Engagement—*100 multiple-choice questions—2 hours and 45 minutes*

A. CONDUCT ENGAGEMENTS (25–35%)	LEVEL P
1. Research and apply appropriate standards: a. IIA Professional Practices Framework (Code of Ethics, Standards, Practice Advisories) b. Other professional., legal, and regulatory standards 2. Maintain an awareness of the potential for fraud when conducting an engagement. a. Notice indicators or symptoms of fraud. b. Design appropriate engagement steps to address significant risk of fraud. c. Employ audit tests to detect fraud. d. Determine if any suspected fraud merits investigation. 3. Collect data. 4. Evaluate the relevance, sufficiency, and competence of evidence. 5. Analyze and interpret data. 6. Develop work papers. 7. Review work papers. 8. Communicate interim progress. 9. Draw conclusions. 10. Develop recommendations when appropriate. 11. Report engagement results. a. Conduct exit conference. b. Prepare report or other communication. c. Approve engagement report. d. Determine distribution of report. e. Obtain management response to report. 12. Conduct client satisfaction survey. 13. Complete performance appraisals of engagement staff.	

EXHIBIT 27.1 CIA Examination Summary (*Continued*)

B. CONDUCT SPECIFIC ENGAGEMENTS (25–35%)	LEVEL P
1. Conduct assurance engagements. a. Fraud investigation 1) Determine appropriate parties to be involved with investigation. 2) Establish facts and extent of fraud (e.g., interviews, interrogations and data analysis). 3) Report outcomes to appropriate parties. 4) Complete a process review to improve controls to prevent fraud and recommend changes. b. Risk and control self-assessment 1) Facilitated approach (a) Client-facilitated (b) Audit-facilitated 2) Questionnaire approach 3) Self-certification approach c. Audits of third parties and contract auditing d. Quality audit engagements e. Due diligence audit engagements f. Security audit engagements g. Privacy audit engagements h. Performance (key performance indicators) audit engagements i. Operational (efficiency and effectiveness) audit engagements j. Financial audit engagements k. Information technology (IT) audit engagements 1) Operating systems (a) Mainframe (b) Workstations (c) Server 2) Application development (a) Application authentication (b) Systems development methodology (c) Change control (d) End user computing 3) Data and network communications/connections (e.g., LAN, VAN, and WAN) 4) Voice communications 5) System security (e.g., firewalls, access control) 6) Contingency planning 7) Databases 8) Functional areas of IT operations (e.g., data center operations) 9) Web infrastructure 10) Software licensing 11) Electronic funds transfer (EFT) and Electronic data interchange (EDI) 12) e-Commerce 13) Information protection (e.g., viruses, privacy) 14) Encryption 15) Enterprise-wide resource planning (ERP) software (e.g., SAP R/3) i. Compliance audit engagements 2. Conduct consulting engagements. a. Internal control training b. Business process review c. Benchmarking d. Information technology (IT) and systems development e. Design of performance measurement systems	
C. MONITOR ENGAGEMENT OUTCOMES (5–15%)	**LEVEL P**
1. Determine appropriate follow-up activity by the internal audit activity. 2. Identify appropriate method to monitor engagement outcomes. 3. Conduct follow-up activity. 4. Communicate monitoring plan and results.	
D. FRAUD KNOWLEDGE ELEMENTS (5–15%)	**LEVELS**
1. Discovery sampling 2. Interrogation techniques	A A

EXHIBIT 27.1 CIA Examination Summary (*Continued*)

3. Forensic auditing	A
4. Use of computers in analyzing data	P
5. Red flag	P
6. Types of fraud	P

E. ENGAGEMENT TOOLS (15–25%)	LEVELS
1. Sampling	A
a. Non-statistical (judgmental)	
b. Statistical	
2. Statistical analyses (process control techniques)	A
3. Data gathering tools	P
a. Interviewing	
b. Questionnaires	
c. Checklists	
4. Analytical review techniques	P
a. Ratio estimation	
b. Variance analysis (e.g., budget vs. actual)	
c. Other reasonableness tests	
5. Observation	P
6. Problem solving	P
7. Risk and control self-assessment (CSA)	A
8. Computerized audit tools and techniques	P
a. Embedded audit modules	
b. Data extraction techniques	
c. Generalized audit software (e.g., ACL, IDEA)	
d. Spreadsheet analysis	
e. Automated work papers (e.g., Lotus Notes, Auditor Assistant)	
9. Process mapping including flowcharting	P

Part III: Business Analysis and Information Technology—*100 multiple-choice questions—2 hours and 45 minutes*

A. BUSINESS PROCESSES (15–25%)	LEVELS
1. Quality management (e.g., TQM)	A
2. The International Organization for Standardization (ISO) framework	A
3. Forecasting	A
4. Project management techniques	P
5. Business process analysis (e.g., workflow analysis and bottleneck management, theory constraints)	P
6. Inventory management techniques and concepts	P
7. Marketing—pricing objectives and policies	A
8. Marketing—supply chain management	A
9. Human Resources (Individual performance management and measurement; supervision; environmental factors that affect performance; facilitation techniques; personnel sourcing/staffing; training and development; safety)	P
10. Balanced scorecard	A

B. FINANCIAL ACCOUNTING AND FINANCE (15–25%)	LEVELS
1. Basic concepts and underlying principles of financial accounting (e.g., statements, terminology, relationships)	P
2. Intermediate concepts of financial accounting (e.g., bonds, leases, pensions, intangible assets, R&D)	A
3. Advanced concepts of financial accounting (e.g., consolidation, partnerships, foreign currency transactions)	A
4. Financial statement analysis	P
5. Cost of capital evaluation	A
6. Types of debt and equity	A
7. Financial instruments (e.g., derivatives)	A
8. Cash management (treasury functions)	A
9. Valuation models	A
a. Inventory valuation	
b. Business valuation	
10. Business development life cycles	A

EXHIBIT 27.1 CIA Examination Summary (*Continued*)

C. MANAGERIAL ACCOUNTING (10–20%)	LEVELS
1. Cost concepts (e.g., absorption, variable, fixed)	P
2. Capital budgeting	A
3. Operating budget	P
4. Transfer pricing	A
5. Cost-volume-profit analysis	A
6. Relevant cost	A
7. Costing systems (e.g., activity-based, standard)	A
8. Responsibility accounting	A

D. REGULATORY, LEGAL, AND ECONOMICS (5–15%)	LEVEL A
1. Impact of government legislation and regulation on business	
2. Trade legislation and regulations	
3. Taxation schemes	
4. Contracts	
5. Nature and rules of legal evidence	
6. Key economic indicators	

E. INFORMATION TECHNOLOGY - IT (30–40%)	LEVEL A
1. Control frameworks (e.g., eSAC, CobiT)	
2. Data and network communications/connections (e.g., LAN, VAN, and WAN)	
3. Electronic funds transfer (EFT)	
4. e-Commerce	
5. Electronic data interchange (EDI)	
6. Functional areas of IT operations (e.g., data center operations)	
7. Encryption	
8. Information protection (e.g. viruses, privacy)	
9. Evaluate investment in IT (cost of ownership)	
10. Enterprise-wide resource planning (ERP) software (e.g., SAP R/3)	
11. Operating systems	
12. Application development	
13. Voice communications	
14. Contingency planning	
15. Systems security (e.g. firewalls, access control)	
16. Databases	
17. Software licensing	
18. Web infrastructure	

Part IV: Business Management Skills—*100 multiple-choice questions—2 hours and 45 minutes*

A. STRATEGIC MANAGEMENT (20–30%)	LEVEL A
1. Global analytical techniques	
a. Structural analysis of industries	
b. Competitive strategies (e.g., Porter's model)	
c. Competitive analysis	
d. Market signals	
e. Industry evolution	
2. Industry environments	
a. Competitive strategies related to:	
1) Fragmented industries	
2) Emerging industries	
3) Declining industries	
b. Competition in global industries	
1) Sources/impediments	
2) Evolution of global markets	
3) Strategic alternatives	
4) Trends affecting competition	
3. Strategic decisions	
a. Analysis of integration strategies	
b. Capacity expansion	
c. Entry into new businesses	
4. Portfolio techniques of competitive analysis	
5. Product life cycles	

EXHIBIT 27.1 CIA Examination Summary (*Continued*)

B. GLOBAL BUSINESS ENVIRONMENTS (15–25%)	LEVEL A
1. Cultural/legal/political environments a. Balancing global requirements and local imperatives b. Global mindsets (personal characteristics/competencies) c. Sources and methods for managing complexities and contradictions d. Managing multicultural teams 2. Economic/financial environments a. Global, multinational, international, and multilocal compared and contrasted b. Requirements for entering the global market place c. Creating organizational adaptability d. Managing training and development.	
C. ORGANIZATIONAL BEHAVIOR (20–30%)	**LEVEL A**
1. Motivation a. Relevance and implication of various theories b. Impact of job design, rewards, work schedules, etc. 2. Communication a. The process b. Organizational dynamics c. Impact of computerization 3. Performance a. Productivity b. Effectiveness 4. Structure a. Centralized/decentralized b. Departmentalization c. New configurations (e.g., hourglass, cluster, network)	
D. MANAGEMENT SKILLS (20–30%)	**LEVEL A**
1. Group dynamics a. Traits (e.g., cohesiveness, roles, norms, groupthink) b. Stages of group development c. Organizational politics d. Criteria and determinants of effectiveness 2. Team building a. Methods used in team building b. Assessing team performance 3. Leadership skills a. Theories compared and contrasted b. Leadership grid (topology of leadership styles) c. Mentoring 4. Personal time management	
E. NEGOTIATING (5–15%)	**LEVEL A**
1. Conflict resolution a. Competitive/cooperative b. Compromise, forcing, smoothing, etc. 2. Added-value negotiating a. Description b. Specific steps	

EXHIBIT 27.1 CIA Examination Summary (*Continued*)

understanding of the CobiT framework should be a CBOK requirement for many if not all internal auditors.

While professionals can quibble about the extent of proficiency or awareness knowledge required for an internal auditor to become a CIA, the topics outlined in Exhibit 27.1 represent a comprehensive CBOK requirement for all internal auditors. These same subject areas are generally covered in the chapters throughout this book, and internal auditors should consider preparing for and taking the CIA examination to demonstrate their knowledge and understanding.

(b) Maintaining Your CIA Certification

An internal auditor does not have to be a member of the IIA to take the CIA examination, although the IIA strongly encourages membership. All CIAs, IIA members and nonmembers, must be familiar with and agree to abide by the IIA's *International Standards for the Professional Practice of Internal Auditing* as well as the IIA's code of ethics. These two, outlined in Chapter 8, set the standards of practice and conduct for all internal auditors. These IIA standards were revised in 2009 from internal auditor best practices, where the guidance said that an internal auditor "should" to an important new internal audit standards requirement specifying that an internal auditor "must."

Upon certification, CIAs are required to maintain their knowledge and skills and to stay abreast of improvements and developments in internal auditing standards, procedures, and techniques. Practicing CIAs must complete and report 80 CPE hours of CPE credits every two years. CIAs must report their CPE activities to the IIA per published deadlines. Those who fail to meet these requirements by the reporting deadline will be placed in inactive status and may not use their designation.

The CIA is a worldwide certification and differs with the CPA, a U.S. certification, or various national versions of chartered accountant certifications. The CIA is the only internationally recognized designation for internal auditors. The CIA examination is offered in English, French, Spanish, Mandarin Chinese, Czech, German, Hebrew, Italian, Japanese, and Portuguese, among others. In the past, candidates had to present themselves at testing sites for proctored sit-down examinations; today the CIA is offered through a worldwide chain of computer-based testing (CBT) sites. A candidate must meet registration requirements, receive a testing site "ticket," and then arrange to visit an authorized testing site. (More information on the CIA process can be found on the IIA Web site, www.theiia.org.)

27.2 Beyond the CIA: Other IIA Certifications

In addition to the CIA, the IIA's Board of Regents offers several other professional certification examinations and certificates: the Certification in Control Self-Assessment (CCSA), the Certified Government Auditing Professional (CGAP), and the Certified Financial Services Auditor (CFSA). These are separate examinations of 125 multiple-choice questions lasting 3 hours and 15 minutes each. Any of these three can be taken as a substitute for Part IV of the regular CIA examination. Each is also offered through the same CBT testing facilities as the CIA examination.

(a) CCSA® Requirements

Chapter 11 describes the IIA's Control Self-Assessment (CSA) process. The CCSA® exam tests a candidate's understanding of important CSA fundamentals, processes, and related topics such as risk, controls, and business objectives. As a means to promote and encourage CSA-related activities, the IIA has established this CCSA professional certification. In contrast to the experience requirements and overall rigor of the CIA examination, the CCSA is a single 3-hour, 125-question examination that tests candidates for their knowledge of CSA processes in six broad domain areas:

Domain 1. CSA Fundamentals (5–10 percent)
Domain 2. CSA Program Integration (15–25 percent)
Domain 3. Elements of the CSA Process (15–25 percent)
Domain 4. Business Objectives/Organizational Performance (10–15 percent)
Domain 5. Risk Identification and Assessment (15–20 percent)
Domain 6. Control Theory and Application (20–25 percent)

Each of these domain testing areas requires the CCSA candidate to demonstrate CSA process knowledge in much more detail than is presented in Chapter 11 of this text. The examination is based on the same topic proficiency and awareness approaches found in the CIA examination. Based on information published in the IIA Web site, Exhibit 27.2 shows an example of the examination's knowledge requirements for just the CCSA Domain 3 area. The topics tested on the CCSA exam are framed in the context of a variety of industry situations. Candidates are not expected to be familiar with industry-specific internal controls but should be able to understand the risks and controls that generally apply to business processes in various industries. The IIA Web site also contains some sample CCSA examination questions. After completion of the CCSA examination, the successful candidate should be able to serve as an experienced CSA session facilitator, as discussed in Chapter 11.

Candidates for the CCSA are not required to have CIA credentials or even to be internal auditors. The experience requirements for the CCSA are that a candidate must have had a strong level of experience in the control self-assessment field. Other requirements, however, such as accepting the code of ethics and continuing education, are similar to those for the CIA. The CCSA alone will give a practitioner a level of expertise in this area, but it should be combined with another certification, such as the CIA. Completion of the CCSA examination also can serve as an alternative substitute for Part IV of the regular CIA examination.

(b) CGAP® Requirements

There are numerous references throughout this book to government auditors but no explanation of their tasks and skills. Whether working for one of the many branches of the U.S. government or at a state or local level, internal auditors face a different set of knowledge and skill requirements from typical internal auditors working the private sector. Attainment of the CGAP allows a candidate to demonstrate these government auditing skills.

CGAP is a specialty certification designed for and by government auditing practitioners. This examination is available in the United States only at this time. It tests a candidate's comprehension of government auditing practices, methodologies, and environment as well as related standards and control/risk models.

EXHIBIT 27.2 CCSA Examination Domain 3 Topics

CCSA Examination Sample Domain Topic Outline
Note: Domain 3 is one of the six topic areas in the CCSA examination. This domain covers about 20% of the test's overall content. The listed areas are domain content areas where a candidate will be expected to have either a P (proficiency) or A (awareness) of the subject area.

Domain 3—Elements of the CSA Process

- **A.** Management's priorities and concerns (P)
- **B.** Project and logistics management (P)
- **C.** Business objectives, processes, challenges, and threats for the area under review (P)
- **D.** Resource identification and allocation (A)
  - **1.** Participants
  - **2.** CSA team
- **E.** Culture of area under review (P)
- **F.** Question development techniques (P)
- **G.** Technology supporting the CSA process (P)
- **H.** Facilitation techniques and tools (P)
- **I.** Group dynamics (P)
- **J.** Fraud awareness (A)
  - **1.** Red flags/symptoms of fraud
  - **2.** Communication and investigation channels
  - **3.** Responding to evidence
- **K.** Evaluation/analytical tools and techniques (trend analysis, data synthesis, scenarios) (A)
- **L.** Formulating recommendations or actions plans (practical, feasible, cost effective) (P)
- **M.** Nature of evidence (sufficiency, relevance, adequacy) (A)
- **N.** Reporting techniques and considerations (types, audience, sensitive issues, access to information) (P)
- **O.** Motivational techniques (creating support and commitment for recommendations) (A)
- **P.** Monitoring, tracking, and follow-up techniques (A)
- **Q.** Awareness of legal, regulatory, and ethical considerations (A)
- **R.** Measuring CSA program effectiveness (A)

The requirements for the CGAP are similar to the CIA and CCSA just described. Candidates for this 3-hour and 15-minute examination must have had two years of auditing experience in a government environment (federal, state/provincial, local, quasi-governmental areas, authority/crown corporation). Work experience must be verified by a CGAP, a CIA, a CCSA, a CFSA, or the candidate's supervisor. The CGAP examination and approximate concentration of questions covers these domains:

Domain 1. Standards and Control/Risk Models (5–10 percent)
Domain 2. Government Auditing Practice (35–45 percent)
Domain 3. Government Auditing Methodologies and Skills (20–25 percent)
Domain 4. Government Auditing Environment (25–35 percent)

This book does not cover the specialized field of governmental internal auditing, but Exhibit 27.3 shows five sample CGAP questions, taken from the IIA Web site. These topics have not been discussed throughout this book, and they show the specialized knowledge requirements of government auditors. The IIA lists a series of reference sources to help a candidate prepare for the CGAP examination.

EXHIBIT 27.3 CGAP Examination Sample Questions

1. In a financial statement audit, Government Auditing Standards (Yellow Book) require that the scope of the review of compliance and internal control over financial reporting be specifically communicated to all of the following EXCEPT the:
   (A) audit client.
   (B) audit committee.
   (C) requestor of audit services.
   (D) funding agency.
2. It is important that an internal audit department's statement of purpose, authority, and responsibility detail:
   (A) the delineation of responsibilities between the internal and external auditors.
   (B) the organizational status of the internal audit function.
   (C) whether the agency head will present audit findings to the oversight committee.
   (D) under what circumstances the internal audit director may have confidential access to the oversight committee.
3. A meter-reading audit for a municipal utility includes the following audit program steps:
   - Determine whether meter readings used in customer billings are free of significant error.
   - Analyze the average read time per day for each meter reader.
   - Review controls over the accurate transmission of meter-reading data from handheld devices to the organization's computer.

   Which of the following types of audit services are included in these audit program steps?
   I. efficiency audits
   II. information technology audits
   III. financial statement audits
   IV. quality audits
      (A) I only
      (B) I and IV only
      (C) II and III only
      (D) I, II, and IV only
4. An internal auditing department plans to begin an audit of a city's highway maintenance department. One of the audit objectives is to determine whether fixed assets employed in highway maintenance are properly reflected in the accounting records. In meeting this objective, which of the following audit approaches is likely to be most effective?
   (A) inspecting fixed assets used in the highway maintenance process and tracing to the asset subsidiary ledger
   (B) scanning the asset subsidiary ledger for credit entries
   (C) selecting items from the asset subsidiary ledger and recalculating depreciation
   (D) examining documentation concerning the cost of fixed assets used in the highway maintenance process
5. Which would be part of the compliance segment of a performance audit?
   (A) Performance reports comply with reporting guidelines.
   (B) Laws and regulations significant to the entity are being followed.
   (C) Activities required by law or policy are being carried out.
   (D) Laws and regulations significant to the audit objective are being followed.

(c) CFSA® Requirements

The CFSA is another of the IIA's specialty certifications and is tailored to demonstrate an individual internal auditor's competence and professionalism in banking, insurance, and securities financial services areas. Candidates may choose any one of these disciplines when taking the exam, regardless of their current occupational field. This exam is available in the United States and Canada only at this time. The examination covers these domain areas:

Domain 1. Financial Services Auditing (25–35 percent)
Domain 2. Banking (25–35 percent)
Domain 3. Insurance (25–35 percent)
Domain 4. Securities (10–20 percent)

The specialized knowledge requirements in each of these financial domains are very different. Exhibit 27.4 shows the application topic outline for insurance—a broad range of topics. Because of very specialized country-by-country rules and practices, the CFSA examination is currently limited to the United States and Canada. It has recently moved to a CBT format but still is only offered in English and only for specific U.S. and Canada national rules. An interested candidate should check with the IIA regarding current country-by-country applicability.

The topics in Exhibit 27.4 were copied from the IIA CFSA Website and illustrate why questions here must be oriented to specific country rules and practices. For example, there is a reference to a need for knowledge of the National Associaton of Insurance Commissioners (NAIC) rules and processes. That reference is for the state-by-state NAIC, procedures that are applicable only for the United States.

(d) Importance of the CIA Specialty Certification Examinations

While the CIA examination and its professional designation are very important for internal auditors as professionals and for managers reviewing the credentials of their internal auditors, there may be limited professional value for these IIA specialty certifications for many internal auditors. For example, the CFSA is a new designation that is not widely recognized, and an internal auditor claiming such credentials may not impress too many people at this time.

However, achieving a CFSA or a CCSA designation can be important for internal auditors working in those specialized areas. They can also complete Part IV of a CIA examination by taking one of these specialty examinations. For an internal auditor working in a government environment at any level, for example, a CIA along with a CGAP could be very valuable.

The overall CIA examination should be an important test and measurement for all internal auditors. Knowledge of the CIA topic areas, as summarized in Exhibit 27.1, also is an excellent set of CBOK requirements for internal auditors. All internal auditors should consider achieving the CIA as a prime professional objective.

27.3 Certified Information Systems Auditor (CISA) Requirements

Previous chapters have mentioned the rivalry between the IIA and what was once the EDP Auditors Association (now the Information Systems Audit and Control

EXHIBIT 27.4 CFSA Examination Topic Outline for Domain 3 U.S. Insurance

CFSA Examination U.S. Insurance Industry Topics

A. Applications/Processes
   1. Marketing, Sales and Distribution
   2. Underwriting
   3. Reinsurance
   4. Actuarial
   5. Claims
   6. Financial Reporting
   7. Compliance
   8. Investment Operations
   9. Risk Management
   10. Premium Audit
   11. Administration

B. Laws and Regulations
   1. The McCarran Ferguson Act
   2. State Insurance Commissions
   3. The NAIC
   4. The Securities and Exchange Commission
   5. ERISA
   6. State Model Laws

C. Products
   1. Life, Pension and Annuity
      a. Individual Insurance
         i) Whole Life
         ii) Term Life
         iii) Universal Life
         iv) Endowments
      b. Group Insurance
         i) Life
         ii) Accident and Health
         iii) Accidental Death and Dismemberment
         iv) Disability
         v) Dental
         vi) HMOs
         vii) Managed Care
         viii) Utilization Management
         ix) Preferred Provider Organizations
         x) Administrative Service Only
      c. Pensions
         i) Qualified Plans
         ii) Tax Favored Individual Retirement Plans
         iii) Qualification Rules
         iv) Plan Discrimination
         v) Savings Plans
         vi) Vesting
         vii) Fiduciaries
         viii) Prohibited Transactions
         ix) Annuity
         x) Fixed Annuities
         xi) Variable Annuities
      d. Reinsurance

EXHIBIT 27.4 CFSA Examination Topic Outline for Domain 3 U.S. Insurance (*Continued*)

2. Property and Casualty Products
   a. Workers Compensation
   b. General Liability
   c. Automobile
   d. Homeowners
   e. Umbrella Coverage
   f. Financial Guarantees
   g. Other

Association [ISACA®]). As mentioned, what is now ISACA was founded by internal auditors who felt the IIA was not giving enough attention to technology and information systems (IS) or information technology [IT] issues. Over the years, these two professional groups have been operating in a somewhat parallel manner, and ISACA has a certification examination similar to but much more IT focused than the IIA's CIA, the CISA examination, and the professional designation. The CISA examination is open to all individuals who have an interest and skills in IS audit, control, and security. The examination is four hours in duration and consists of 200 multiple-choice questions. The test is offered each year in June and December at many locations worldwide.

In addition to passing the CISA examination, a candidate must have a minimum of five years of professional IS auditing, control, or security-related work experience. A maximum of one year of IS experience *or* one year of financial or operational auditing experience can be substituted for one of those five years of IS auditing, control, or security experience. In addition, 60 to 120 completed college semester credit hours (the equivalent of an associate or bachelor's degree) can be substituted for one or two years, respectively, of IS auditing, control, or security experience. Also, two years as a full-time university instructor in a related field (e.g., computer science, accounting, IS auditing) can be substituted for one year of IS auditing, control, or security experience.

This experience must have been gained within the 10-year period preceding the application date for certification or within 5 years from the date of initially passing the examination. Retaking and passing the examination will be required if the application for certification is not submitted within 5 years from the passing date of the examination. All experience is verified independently with employers.

Per ISACA guidelines, the tasks and knowledge required of ISsystems audit professionals serve as the blueprint for the CISA examination. Exhibit 27.5 shows the six broad subject areas included in the CISA examination. More information about the requirements in each of these knowledge areas can be found in the ISACA Web site (www.isaca.org) or in a variety of reference materials listed there as well. That same Web site contains a set of test sample questions.

The CISA examination has similar education, experience, and continuing education requirements as for the CIA examination discussed previously. This is a fairly technical level of examination, and even though a candidate may have achieved CIA certification, the CISA requires technical knowledge in an extensive set of areas.

EXHIBIT 27.5 CISA Examination Content Areas

1. **IS Audit Process (10%)**
   Provide IS audit services in accordance with IS audit standards, guidelines, and best practices to assist the enterprise in ensuring that its information technology and business systems are protected and controlled.
2. **IT Governance (15%)**
   Provide assurance that the organization has the structure, policies, accountability, mechanisms, and monitoring practices in place to achieve the requirements of corporate governance of IT.
3. **Systems and Infrastructure Life Cycle (16%)**
   Provide assurance that the IT service management practices for the development/acquisition, testing, implementation, maintenance, and disposal of systems and infrastructure will meet the enterprise's objectives.
4. **IT Service Delivery and Support (14%)**
   Provide assurance that the IT service management practices will ensure delivery of the level of services required to meet the enterprise's objectives.
5. **Protection of Information Assets (31%)**
   Provide assurance that the security architecture (policies, standards, procedures, and controls) ensures the confidentially, integrity, and availability of information assets.
6. **Business Continuity and Disaster Recovery (14%)**
   Provide assurance that, in the event of a disruption, the business continuity and disaster recovery processes will ensure the timely resumption of IT services while minimizing the business impact.

The CISA designation has been a globally accepted standard of achievement in the IS audit, control, and security field since 1978 and has been recognized by many governments and major business groups around the world. More than 40,000 people have attained the CISA certification since its inception in the 1980s.

27.4 Certified Information Security Manager® Certification

ISACA also offers a second and relatively new certification and examination, the Certified Information Security Manager (CISM). This program was launched in 2004. A base of certified CISMs was established by grandfathering in professionals who already had strong levels of IS security experience. The CISM program is very similar to the CISSP examination.

The CISM exam is offered two times per year and covers five information security management areas. This examination covers the work performed by information security managers, as validated by prominent industry leaders, subject matter experts, and industry practitioners. These areas and the approximate percentage of test questions allocated to each one are:

- Information Security Governance (23 percent)
- Information Risk Management (22 percent)
- Information Security Program Development (17 percent)
- Information Security Program Management (24 percent)
- Incident Management and Response (14 percent)

The ISACA Web site presents a fairly detailed outline of areas that a CISM manager would be expected to perform and know. The requirements for taking this worldwide certification examination are similar to the CISA, although it is not offered yet in many languages.

The CISM is a new test and certification with little track record today. Because it is supported by the very strong and credible ISACA organization, we can expect to see it grow in terms of status and recognition. However, these examinations and certifications often take time to become highly recognized among managers and professionals. While preparing and sitting for any professional examination is an excellent learning exercise for any professional, an internal auditor may want to wait to see how widely the CISM is recognized before taking this examination. Exhibit 27.6 describes the knowledge requirements for the CISM examination.

27.5 Certified Fraud Examiner

Concerns regarding fraud and fraud investigations are becoming increasingly important to all auditors. Chapter 25 discusses fraud detection and prevention and highlights how, in the past, both external and internal auditors felt that investigating and detecting fraud was not their responsibility. However, in the post–Sarbanes-Oxley Act (SOx) era, internal and external auditors have a strong responsibility to investigate for fraud and to take appropriate actions when it is identified.

The Association of Certified Fraud Examiners (ACFE) is the professional organization that is very involved with fraud-related issues for the internal auditor. The organization has its own professional examination and certification, the Certified Fraud Examiner (CFE). Obtaining a CFE designation is regarded as an indicator of excellence in the antifraud profession. CFE members can position themselves as leaders in the antifraud community.

The CFE examination is based on four broad areas:

1. Criminology and Ethics
2. Financial Transactions
3. Legal Elements of Fraud
4. Fraud Examination and Investigation

These are topic areas beyond the experience and training of many internal auditors. The ACFE, of course, has its own publications, conferences, and local chapters to provide internal auditors with a greater level of information about fraud and fraud investigations.

Although a relatively new professional organization, the ACFE has quickly gained prominence in the post-SOx era. The ACFE has its own Web site (www.acfe.com). Much of the fraud material published on the American Institute of Certified Public Accountants Web pages on fraud and valuation services (//fvs.aicpa.org/) and discussed in Chapter 25 is based on ACFE materials. In addition, the ACFE Web site contains a sample examination to allow an internal auditor to determine if he or she is ready to take the CFE test. The CFE test is an entirely online exercise; candidates register and start taking the examination over an online timed process.

EXHIBIT 27.6 CISM Tasks and Knowledge Statements Example

Note: These are knowledge areas for one area or domain in the CISM examination, as published on the ISACA Web site in 2008. The represent responsibilities and key knowledge requirements of an information security manager for the CISM examination but may be subject to change as the examination is revised over time. For more information, see www.isaca.org.

Tasks

1.1 Develop an information security strategy aligned with business goals and objectives.
1.2 Align information security strategy with corporate governance.
1.3 Develop business cases justifying investment in information security.
1.4 Identify current and potential legal and regulatory requirements affecting information security.
1.5 Identify drivers affecting the organization (e.g., technology, business environment, risk tolerance, geographic location) and their impact on information security.
1.6 Obtain senior management commitment to information security.
1.7 Define roles and responsibilities for information security throughout the organization.
1.8 Establish internal and external reporting and communication channels that support information security.

Knowledge Statements

1.1 Knowledge of business goals and objectives
1.2 Knowledge of information security concepts
1.3 Knowledge of the components that comprise an information security strategy (e.g., processes, people, technologies, architectures)
1.4 Knowledge of the relationship between information security and business functions
1.5 Knowledge of the scope and charter of information security governance
1.6 Knowledge of the concepts of corporation and information security governance
1.7 Knowledge of methods of integrating information security governance into the overall enterprise governance framework
1.8 Knowledge of budgetary planning strategies and reporting methods
1.9 Knowledge of business case development
1.10 Knowledge of the types and impact of internal and external drivers (e.g., technology, business environment, risk tolerance) that may affect organizations and information security
1.11 Knowledge of regulatory requirements and their potential business impact from an information security standpoint
1.12 Knowledge of common liability management strategies and insurance options (e.g., crime or fidelity insurance, business interruptions)
1.13 Knowledge of third party relationships and their impact on information security (e.g., mergers and acquisitions)
1.14 Knowledge of methods used to obtain senior management commitment to information security
1.15 Knowledge of the establishment and operation of an information security steering group
1.16 Knowledge of information security management roles, responsibilities and general organizational structures
1.17 Knowledge of approaches for linking policies to enterprise business objectives
1.18 Knowledge of generally accepted international standards for information security management
1.19 Knowledge of centralized and distributed methods of coordinating information security activities
1.20 Knowledge of methods for establishing reporting and communication channels throughout an organization

27.6 CISSP Information Systems Security Professional Certification

A professional organization know as the International Information Systems Security Certification Consortium or $(ISC)^2$ is responsible for one of the more challenging and better-recognized internal audit–related professional certifications and examinations, that of the Certified Information System Security Professional (CISSP). This professional examination and designation are not achieved by many. This is really a certification for IS security professionals, not ordinary internal auditors.

With the possible exception of the CISM examination, the CISSP examination is on a much higher, much more technical level than the other internal auditor certification examinations discussed in this chapter. The CISSP exams are closely proctored, training materials are reviewed and approved by $(ISC)^2$, and the overall quality of the examination is high. People with a CISSP certification almost certainly have a high knowledge of IS security.

27.7 ASQ Internal Audit Certifications

Chapter 31 discusses the American Society for Quality (ASQ) and its quality auditor certifications. The ASQ sponsors a wide range of examinations and certifications for all aspects of its operations, including the Certified Quality Auditor (CQA) examination and certification. A CQA is a professional who understands the standards and principles of quality management auditing and the techniques of examining, questioning, evaluating, and reporting to determine a quality system's adequacy and deficiencies. The CQA analyzes all elements of a quality system and judges its degree of adherence to the criteria of industrial management and quality evaluation and control systems. The difference between a regular internal auditor and a CQA is that the latter often works in a quality assurance group and spends more time on process-oriented reviews as opposed to the IIA internal auditor's financial and operational reviews. CQA auditors often work in production areas and perform more hands hands-on reviews than CIA-level internal auditors.

There are both differences and similarities between the IIA-heritage internal auditors who are the subject of many of these chapters and ASQ quality auditors discussed in Chapter 31. While many ASQ auditors also are IIA members, they often seek their own professional CQA certification. To achieve quality auditor certification, the candidate is required to pass a five-hour, multiple-choice written examination that measures comprehension of the quality audit profession. As the minimum professional expectations, a CQA quality auditor must:

- Possess the knowledge to effectively conduct different types of objective, ethically based audits using and interpreting applicable standards/requirements.
- Be able to develop and communicate an audit plan within a defined scope that identifies applicable standards, necessary personnel, required documents and tools, and an audit agenda.
- Be able to effectively execute an audit plan, including the opening meeting, performing the audit, and the closing meeting using generally accepted auditing techniques and verifying, documenting, and communicating findings as appropriate for the audit.

- Be able to objectively present verified nonconformance to the audited standard and evaluate the effectiveness of the resulting follow-up/corrective action activities in an ethical and timely manner.
- Know and be able to apply basic auditing tools and techniques, such as flowcharting, the concept of variation, observation techniques, and physical examination techniques. A CQA must also demonstrate a general knowledge of quality control tools, descriptive statistics, and applicable sampling theories.

The CQA requirements are similar to those of the IIA-oriented internal auditor, but the CQA uses different approaches and terminology. For example, the last list mentions "verified nonconformance to the audited standard" and "the concept of variation." These are specialized ASQ terms, although many other concepts go back to standard IIA internal audit processes. The CQA examination is based on the ASQ's Body of Knowledge, a comprehensive set of key knowledge areas and practices for the CQA. This body of knowledge document is maintained by the ASQ professional organization.

A CSQ-certified auditor has similar professional and continuing education requirements as a CIA. If nothing else, the ASQ's rules are perhaps more stringent than the IIA and require the recertification of all CSQs every three years. Professionals who have not completed required continuing educational requirements must retake the CSQ examination to regain their certification.

The ASQ has two other specialized Quality Auditor certifications, one for biomedical quality audits and the other for Hazard Analysis and Critical Control Point or HACCP-based (or process-safety) systems. The ASQ is very responsive to member requests to build a separate certification when there appears to be a special demand. This ASQ practice is just a different area of quality auditing.

27.8 Other Internal Auditor Certifications

As discussed at the beginning of this chapter, some professions have a large number of professional certification available to them, depending on an internal auditor's job requirements and skills. The certification depends on the auditor's needs and interests. The requirements for all certifications are similar, usually consisting of specified requirements to take the examination, pass it, and receive the "Certified" designation, followed by continuing education requirements to keep the certification current.

A professional certification is a good way for internal auditors to demonstrate that they have some unique and important professional skills. Professional certifications are important. The knowledge gained through obtaining a certificate allows an internal auditor to work more efficiently and effectively in service to management. Certification and in particular the CIA is important for all internal auditors. All internal auditors should make the effort to become certified as CIAs and/or as CISAs. Individual internal auditors should use these certification examinations as a measure of their own professionalism. These are important indicators of one's knowledge, interests, and abilities. Both within an organization's internal audit function or beyond, certifications are measures of one's knowledge and interests in the profession.

We have concluded most of these chapters by discussing the chapter's subject as a strong or more moderate internal auditor CBOK requirement. Every internal auditor

should understand why a professional certification, such as a CIA, is important and should have a general knowledge of what it takes to achieve that certification. A general knowledge of the chapter topics throughout this book should help an internal auditor to achieve some of the general understanding of the necessary requirements for each of the certification discussed here. However, beyond this book, a strong professional auditor should study and become a CIA and/or a CISA or even a CISM.

CHAPTER 28

Internal Auditors as Enterprise Consultants

An internal auditor's role as a business consultant has sometimes been a bit ambiguous. Until recently, the Institute of Internal Auditor's (IIA's) *International Standards for the Professional Practice of Internal Auditing,* as discussed in Chapter 8, prohibited internal auditors from acting as business consultants. The idea had been that an internal auditor was there to review and assess internal controls and then to make recommendations for controls improvements and corrective actions through internal audit reports. The thinking then was that internal audit consulting actions might create a conflict of interest. This no-consulting standard was not followed too closely; many internal auditors often acted like consultants as part of their management-oriented reviews. This author recalls his earlier days as an information technology (IT) internal auditor. With five plus years developing and designing IT applications and a strong understanding of systems development processes, it was difficult to not act as a consultant. Many other internal auditors all but ignored consulting prohibitions when making their internal audit recommendations.

The internal audit consulting prohibition became stronger in the early days of the Sarbanes-Oxley Act (SOx). While the early SOx legislation hardly mentioned internal audit, many felt that internal audit would be in violation of these no-consulting rules if it helped management to install effective Section 404 internal control processes. The rules have since changed, however, and newer IIA standards now expressly *permit* internal auditors to act as management consultants in certain designated and specified audit reviews. Many of the IIA standards are now separated into distinct attest (i.e., auditing) and consulting guidance sections.

This chapter discusses internal audit's potential role as an internal consultant to the auditor's overall enterprise. We discuss the consulting IIA standards and how internal audit consulting services can fit in and interface with otherwise normal internal audit review activities. In addition, we look at how internal audit can deliver internal consulting to the enterprise in a manner that does not conflict its normal audit attest functions.

Serving as an enterprise consultant is an expanded and important role for many internal auditors. Internal consulting may not fit in all internal audit functions. In some cases, the industry, audit committee concerns, or even the size of the internal audit function may restrict any plans to offer internal consulting service. Where these arrangements seem to work, however, internal audit typically has the inside knowledge and experience to be an important and powerful internal consultant. All internal auditors should have a common body of knowledge (CBOK) level

of knowledge of the distinctions between internal audit attest responsibilities and serving as internal consultants. In addition, when internal auditors elect to act as enterprise consultants, they need to have a good CBOK level of understanding of consulting best practices.

28.1 Standards for Internal Audit as an Enterprise Consultant

As mentioned throughout this volume, the purpose of an internal audit is to assist management by providing analysis, information, and recommendations for the improvement of controls and operations. Internal controls may be evaluated for:

- Compliance with policies and procedures, rules, and regulations
- Reliability and integrity of financial and operational information
- Effectiveness and efficiency of operations
- Safeguarding of assets

IIA standards now specifically describe internal auditing as both an attest and a consulting activity. They allow internal auditors to provide consulting services relating to operations for which they had previous responsibilities, provided that they disclose any potential impairment to their independence or objectivity relating to proposed consulting services prior to accepting the engagement.[1] The IIA standards define internal audit consulting as advisory and related to audit client service activities, the nature and scope of which are agreed with the client and which are intended to add value and improve an enterprise's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

There is often a large gap between attest-level internal auditing and what it takes to be an effective consultant. In their internal audit reports, internal auditors may recommend changes, but they cannot ensure that the changes take place. Internal auditors often just perform an attest audit, make recommendations on multiple levels, and then collaborate to make an outcomes better.

Serving as internal consultants, internal auditors can be held to higher standards of performance and accountability. In these situations, they need to act as objective and critical "outsiders" within their own enterprises, delivering the hard facts and bad news beyond audit report findings, including issues that management sometimes does not want to hear. Also, they need to be prepared to deliver the truth to management beyond just errors, omissions, and internal control weaknesses. They also need to be good at off-the-record consulting-related conversations, which are sometimes more important than the written audit report. Internal auditors who master the principles of effective internal consulting can use the related methods and techniques to dig deeper and deliver the truth.

Serving as enterprise consultants often places internal auditors in a rather different role from normal internal audit attest assignments, where internal audit uses its audit planning and risk objective measurements to plan and schedule the audit review. Although management usually has some flexibility in delaying or rescheduling a planned review, internal audit has the authority and responsibility to schedule it. In addition, internal audit can generally define its own scope, time schedules, and audit team assignments. Internal audit scheduling normally operates on a collaborative basis, and local management can negotiate an audit visit or even appeal to

senior management and ultimately the audit committee if they object to a planned internal audit visit, internal audit generally has the responsibility for launching an internal audit review.

Responsibilities for initiating and for scheduling a consulting assignment are often very different. Management engages internal auditors to come and help as consultants in some area. The assignment objectives, timing, assigned team, scope of work to be performed, and almost everything else is subject not to internal audit's plans but to negotiation with the requesting management group. In some respects, when internal audit acts as an enterprise consultant, management seeks it out and engages with internal audit similar to contracting with an outside firm that offers consulting services. A consulting project is launched through a formal engagement letter, as discussed in Section 28.4 and also shown in Exhibit 7.3, and the project often proceeds in an informal, almost collaborative way. Going beyond that old joke by some management skeptics—"Hello, I'm from internal audit, and I'm here to help you"—an internal auditor acting as an enterprise consultant has really been brought in because management has requested that consulting help.

There are also some other significant differences between internal audit operating as an internal consultant and management's use of an outside, independent consulting firm. Perhaps the strongest difference is that if management decides it does not approve of the external consultants, it can fire them. Things are not as easy when using internal audit consulting resources. Although management can end an internal audit consulting engagement, that same audit team still is part of the overall enterprise. On the very positive side, however, internal auditors acting as internal consultants better understand the organization's systems, culture, issues, and a wide range of other matters. An external consultant often does not have such in-depth knowledge.

Internal audit consulting standards now clearly define internal audit's potential role as an internal consultant. However, some members of senior management or the audit committee may not realize that internal audit standards now allow such formal internal consulting activities. An internal audit function needs to plan and formally launch its internal consulting activities. Of course, internal audit should first discuss these arrangements, first with the audit committee. The chief audit executive should describe how this newer, expanded component of internal audit's service to management can bring value to the enterprise. Of course, internal audit should never lose sight that its prime responsibility is to review the adequacy and effectiveness of internal controls in the enterprise. The internal audit attest role is very significant.

28.2 Launching an Internal Audit Internal Consulting Capability

Before engaging in ongoing in-house consulting activities, internal audit needs to receive approval from the audit committee and to fully demonstrate to management that it has the ability and is objective enough to act as an enterprise consultant. The fact that internal audit standards now allow internal audit consulting engagements does not mean that every internal audit function *must* do so. The number of other internal audit opportunities may limit internal audit's ability to perform any consulting activities beyond normal audit attest reviews. In addition, as discussed, some members of management may not fully understand internal audit's potential role as an internal consultant, thinking of it only in an attest role.

If an enterprise's internal audit function wants to begin offering internal consulting, it should develop a consulting strategy and then strongly document that role and their capability through the audit charter. Chapter 12 discussed the importance of audit committee–approved internal audit charters and provided examples. However, because past IIA standards prohibited internal auditors from acting as consultants, this expanded internal audit potential role may not be well understood. The internal audit department itself needs to develop a strategy for internal consulting activities that does not conflict with its main mission—review of internal controls—and that brings value to the overall enterprise. Some areas to consider when developing an internal consulting practice include:

- **What types of internal audit consulting will be considered?** Internal audit may have the skills to perform internal controls reviews in many specialized areas but not have the necessary consulting expertise in those areas. Whether it is helping with new financial transaction processes, improving IT application controls, or even just general documentation, internal audit should clearly understand and define what they can and cannot do well.
- **How will resources be divided between attest-related internal auditing and internal consulting?** Internal audit needs to take extreme care that it is not viewed as auditors one day and consultants the next. In a larger audit enterprise, this can be accomplished by creating a separate internal consulting section within the overall internal audit function. Otherwise, care must be given to separating these two different functions.
- **Budgeting and accounting for costs of internal audit consulting services.** Although external or independent consulting firms typically bill their services at fairly substantial rates, internal audit attest services are often delivered "free" to their enterprises, with costs being covered out of centralized financial budgets. Internal consulting should perhaps be viewed as a value-added function, similar in manner to how an enterprise imposes internal budget charges on graphics or computer time services. A charging and billing mechanism should be established for any such internal consulting activities.
- **Planning and scheduling internal audit consulting activities.** Separate but different planning and scheduling tools should be established for all internal consulting activities. Many of the same procedures for planning and performing internal audits discussed in Chapters 7 through 11 are applicable here. However, internal audit consulting activities should be kept separate from regular internal audit materials.
- **Reporting results and communication with management and the audit committee.** Consulting activities should go through a regular reporting process similar to the basic format of the internal audit reports discussed in Chapter 17. However, consulting reports do not contain the same audit report findings, recommendations, and expected responses found in normal internal audit reports. In addition, often consulting reports do not have to be detailed; high-level summaries are acceptable.
- **"Selling" the internal audit consulting program.** If internal audit is going to provide consulting services to the overall enterprise, it must sell and promote these activities. While we are not suggesting power lunches to promote a program, internal audit should develop an informal services catalog to describe its consulting capabilities and offerings.

There are many options to consider when launching internal audit consulting offering. The listed considerations and others should be outlined and then discussed with both the audit committee and senior management. Once tentative approvals have been obtained, internal audit should request an approved audit charter that clearly specifies its role as an internal consultant to the enterprise. Exhibit 28.1 is an example of an internal audit charter that specifically authorizes internal audit's role as an internal enterprise consultant.

An internal audit internal consulting activity should be a normal offering of internal audit services and not just an ad hoc exercise that occurs only for limited, special-purpose occasions. As an available offering that takes advantage of and builds on internal audit's skill set, internal consulting resources need to be offered and appropriately managed. Internal audit must be aware of its skill set and not get involved with activities that might better belong with other enterprise resources or with outside consultants.

28.3 Ensuring an Audit and Consulting Separation of Duties

Public accounting firms present an example of the need for adequate separation of responsibilities between internal auditors acting as internal consultants and those doing audit attest work. Before the 1970s, the American Institute of Certified Public Accountants separated public accounting firms between CPA auditors and professionals providing consulting services. A public accounting firm then would have sort of a dotted line in the office, separating auditors who certified financial reports from specialists, such as IT consultants. Over the years, however, this dotted line grew fuzzier as specialist consultants, particularly those with IT skills, got directly involved in helping to complete audits of heavy IT-bound enterprises. Similarly, strong CPA financial auditors became very involved in helping with specialized financial consulting projects.

This separation-of-duties barrier really slipped and became almost transparent before the fall of Enron and the passage of SOx in the early twenty-first century. One of the internal control breakdowns highlighted in the SOx legislative hearings was that public accounting firms often strongly suggested that one of its IT consultants visit a financial audit client to install a new financial application; the public accounting firm would send its CPA auditors back to review the internal controls over that same application. Interestingly, the financial auditors typically did not find many internal control problems in the applications their own consultants had just installed. SOx has forbidden this potential conflict-of-interest approach, and public accounting consulting practices have now moved off as independent consulting firms.

The point of this example is to show that separation-of-duties restrictions between auditing and consulting can break down over time. Care must be paid to separating the roles of internal auditors acting as consultants from those performing audit attest functions. Paraphrasing internal audit consulting standards that are summarized in Chapter 8 (see Section 8.2(b), 2201), it is particularly important that internal auditors establish an understanding with consulting engagement clients about objectives, scope, respective responsibilities, and other client expectations. For significant internal audit consulting engagements, this understanding should be documented.

EXHIBIT 28.1 Audit Charter Authorizing Internal Audit Internal Consulting

This charter is very similar to the sample charter for Global Computer Products in Exhibit 12.1. This version specifically authorizes internal audit to engage in internal consulting activities in addition to normal internal audit attest reviews. Consulting-related authorizations are displayed in bold.

Internal Audit's Mission
The mission of Global Computer Products Internal Audit is to ensure that company operations follow high standards both by providing an independent, objective assurance function and by advising and consulting on best practice. By using a systematic and disciplined approach, Internal Audit helps Global Computer Products accomplish its objectives by evaluating and improving the effectiveness of risk management, internal control and governance processes.

Independence and Objectivity
To ensure independence, Internal Audit reports directly to the Board of Directors Audit Committee, and to maintain objectivity, Internal Audit is not involved in day-to-day company operations or internal control procedures. **However, internal audit may provide independent consulting help in certain specifie areas that is independent from regular internal audit review procedures.**

Scope and Responsibilities
The scope of Internal Audit's work includes the review of risk management procedures, internal control, information systems and governance processes. This work also involves periodic testing of transactions, best practice reviews, special investigations, appraisals of legal and regulatory requirements, and measures to help prevent and detect fraud.

To fulfill its responsibilities, Internal Audit shall:

- Identify and assess potential risks to the Bank's operations.
- Review the adequacy of controls established to ensure compliance with policies, plans, procedures, and business objectives.
- Assess the reliability and security of financial and management information and supporting systems and operations that produce this information.
- Assess the means of safeguarding assets.
- Review established processes and propose improvements.
- Appraise the use of resources with regard to economy, efficiency, and effectiveness.
- Follow up recommendations to make sure that effective remedial action is taken.
- Carry out ad hoc appraisals, investigations, or reviews requested by the Audit Committee and Management.
- **Perform independent consulting projects at the specifi request of management** .

Internal Audit's Authority In order to promote effective controls at reasonable cost, Internal Audit is authorized, in the course of its activities, to:

- Enter all areas of Global Computer Products operations, and have access to any documents and records considered necessary for the performance of its functions.
- Require all members of staff and management to supply requested information and explanations within a reasonable period of time.
- Engage in independent consulting reviews at the specific request and authorization of management.

EXHIBIT 28.1 Audit Charter Authorizing Internal Audit Internal Consulting (*Continued*)

Accountability
Internal Audit shall prepare, in liaison with management and the Audit Committee, an annual audit plan that is based on business risks, the results of other internal audits, and input from management. The plan shall be presented to senior management, including the General Counsel, for approval by the Audit Committee. Any needed adjustments to the plan should be communicated to and approved by the Audit Committee.

Internal Audit is responsible for planning, conducting, reporting, and following up on audit projects included in the audit plan and deciding on the scope and timing of these audits. The results of each internal audit will be reported through a detailed audit report that summarizes the objectives and scope of the audit as well as observations and recommendations. In all cases, follow-up work will be undertaken to ensure adequate response to internal audit recommendations. Internal Audit also will submit an annual report to senior management and to the Audit Committee on the results of the audit work, including significant risk exposures and control issues. **Internal Audit also may complete independent consulting projects, at the specifi authorization of management, that are not part of specifi audit report recommendations .**

Standards
Internal Audit adheres to the standards and professional practices published by the Institute of Internal Auditors as well as the Information Technology Governance Institute.

28.4 Consulting Best Practices

Many people do not have a clear understanding of what it means to be a consultant. The person selling shoes at a retail store may have a job title of "sales consultant," and the Web contains many other definitions for a consultant. According to those definitions, a consultant is an individual who provides counsel and assistance to a client on specific assignments. Another more academic-sounding definition of consulting (from the Latin *consultare*) means "to discuss" and refers to a professional who provides advice in a particular area of expertise, such as accountancy, the environment, technology, law, human resources, marketing, medicine, or finance.

The role of a consultant is a little different from that of an internal auditor. An internal auditor starts with a prepared audit program outlining areas to review or a set of standards. Much of the review is based on an assessment of compliance against those standards. As discussed previously, an internal auditor generally schedules a review while a consultant comes at the invitation of management. Consultants may structure a review on the basis of compliance with some standards, but generally they approach assignments more like open books, discussing matters with management and developing solutions in a more collaborative manner.

In order to operate as effective internal consultants, internal auditors need to do more than change their title on a business card; they also need to develop some new approaches. The next sections briefly define some key action steps for internal auditors operating as internal consultants. However, as discussed previously, internal audit should have fully defined its capabilities for consulting work and outlined them through an approved charter statement.

(a) First Steps: Launching a Consulting Assignment

Internal consulting opportunities typically come to internal audit for three reasons:

1. The department has completed an internal review with recommendations for corrective action that management needs help to implement.
2. Other needs develop within the enterprise, such as significant deficiencies requiring correction that were highlighted during the external auditor's SOx Section 404 reviews.
3. Management has some specific needs where internal auditor expertise may be of help.

We generally recommend that internal audit should not actively promote its consulting services beyond these basic areas. It should operate primarily to fulfill specific needs management needs.

(i) CONSULTING HELP TO IMPLEMENT INTERNAL AUDIT REPORT RECOMMENDATIONS A major component of the internal audit process is internal audit's recommendations for corrective action, published and described in an audit report. Internal audit enterprise-specific standards and audit committee direction usually require that auditee management must respond to the audit report findings with a plan for corrective action in a very short time. In some cases, an internal audit finding outlining the need for some form of corrective actions puts a burden on management, which may lack the skilled resources to implement the suggested improvement.

In some situations, internal auditors acting as in-house consultants may be an appropriate resource to implement these audit report recommendations. This is particularly the case when an internal audit recommendation covers such areas as improving documentation, improving certain internal control procedures, or training staff in areas related to internal control. If an auditee's own departmental resources are limited, an internal audit internal consultant may be the best resource to implement the recommended corrective action. Bringing in a new, outside consultant might be much more expensive and time consuming. If auditee management indicates that it does not have the resources available to implement the internal audit recommendations, internal audit's consulting services might be proffered.

There are some major danger areas with this type of consulting work. First, internal audit recommendations should not be self-serving in a manner that appears to build consulting opportunities. Second, there must be a level of independence between the internal auditors who made the recommendation and the internal consultants helping to implement corrective actions. That level of independence should be strong enough such that an internal consultant helping to implement a suggested recommendation should be able to take exception to some area of a recommendation and to point out any shortcomings.

(ii) OTHER CONSULTING NEEDS WITHIN THE ENTERPRISE There are often many areas within an enterprise where internal audit's skills can meet needs and offer some help and expertise. A good example might be when management formally requests help with the SOx Section 404 internal controls compliance review, and internal audit assists. (This process is discussed in Chapter 4.) Similarly, external auditors might have found some significant control weaknesses and have passed these concerns

on to the audit committee and management. Internal audit often has the broad skills to help install internal control improvements not as internal auditors but as management consultants.

(iii) SPECIFIC MANAGEMENT NEEDS FOR INTERNAL AUDIT CONSULTING HELP Internal auditors have wide skill and knowledge areas. Beyond specific internal audit risk-based audit assignments, internal audit often can provide consulting help in a wide variety of areas. Examples might include helping to build effective internal controls in a new IT application, discussed in Chapter 19, or helping to launch an ethics hotline function, as discussed in Chapter 24. By providing internal consulting support, internal audit can be a major help to the overall enterprise.

Any internal audit consulting project depends on management needs, the availability of internal audit resources, and the overall approval of the audit committee. When there is a perceived need or interest, internal audit representatives should meet with the requesting management group to discuss their requirements. The internal audit consultants should gain a high-level understanding of the project's needs and requirements.

This preliminary process usually requires internal auditors as to gather more information about the possible assignment in order to size the issue. For example, say enterprise management wants to better organize the documentation processes that cover its product repair and return operation. With its background in preparing workpaper documentation, internal audit is an obvious choice to provide some help and direction here. However, after some very preliminary discussions, a member of the internal audit team—probably someone who would fill the consultant role—should visit this customer service area to understand the specific nature of the request, the size of problem, and whether an internal audit consultant can be of help. If things appear to be a good match, internal audit should formalize this internal consulting arrangement.

(b) Consulting Engagement Letters

An authority or leader from the internal audit internal consulting team should draft a formal letter of understanding describing the internal consulting project. Because this is an enterprise-level internal understanding, such an engagement letter does not have the same legal basis as one provided by an outside firm. However, a formal engagement letter is an appropriate way to launch an internal consulting project between internal audit and an enterprise operation.

Exhibit 28.2 is an example of an internal audit consulting engagement letter. The document describes what the internal audit consultant proposes to accomplish, who will be doing the work, its timing and duration, and the expected outcomes from the consulting project. If internal audit charges for its consulting services through some form of a budget cross-charge, expected cost factors should also be estimated. An engagement letter launches an internal consulting project and should require appropriate management approval.

The approved engagement letter should then become the basis for launching an internal audit consulting project. Chapter 7 discussed planning and performing a "typical" internal audit, and Chapter 14 discussed internal audit project management. An internal audit consulting project should be organized and tracked in the same manner as a normal internal audit. A major difference, however, is that the consulting

EXHIBIT 28.2 Internal Audit Consulting Engagement Letter Example

Global Computer Products

Internal Audit Consulting

Consulting Engagement Authorization

The finished goods shipping department at the Metroville, PA, plant has identified a need to improve its customer service operations at that facility and has requested that specialists from the corporate internal audit department perform a detailed analysis of plant operations and then lead an effort to improve operations at that facility. Based on this request and on recommendations from a recent internal audit review of this same facility, a team of independent internal audit consultants propose to review these customer service facilities and to help improve controls and procedures as necessary.

A team of consultants, led by consultant Tom Bell, plan to visit the Metroville, PA, plant during February 20XX to perform a detailed independent analysis of operations and to suggest areas for improvement, including the identification and implementation of a new customer service computer system. We expect to complete this analysis and provide recommendations for approval approximately six weeks after the initiation of this project. The final selection and installation of a new computer system will take additional time and resources to be discussed at the time of our preliminary analysis.

We expect this work to require approximately hours, and our charges will be internally billed to your department through the corporate expense accounting system, based on our normal billing rate of $xx per hour as well as any out-of-pocket charges associated with this review. The charges associated with any new custom service computer system will be based on a separate estimate to be presented later.

I recognize that the internal audit consulting group will be operating independent from internal audit review activities, and I authorize them to begin this consulting project as described.

Name: _____ Date: _____

project is subject to local management's request and priorities. If local management tells the internal auditors serving as consultants to ignore some area of operations or to give some discovered problem a pass, the internal auditor consultant does not have the same flexibility in bringing the matter to the attention of the audit committee.

(c) Consulting Process: Defining "As Is" and "To Be" Objectives

Consulting projects are almost always very different from internal audits, where the auditor starts with an audit program or set of standards. In a consulting project, local management typically has an idea that some area of operations is wrong or could be performed more effectively or efficiently. With these broad concepts in place, the internal auditor as consultant needs to analyze the matter and develop a potential problem statement to begin the consulting exercise.

Although many different approaches can be used, a cause-and-effect analysis is a useful approach to analyzing the current status of some problem area. The consultant is presented with a general problem statement and then reviews information, asks

questions, and observes the problem environment to break it down to smaller pieces. For example, if there is a potential problem concerning training, the consultant might consider whether the training responsibilities were formally established, if general needs have been identified, and if appropriate personnel are being brought into the training process.

Assume that an internal auditor consultant has been asked to identify customer service problems in a business unit operation. The consultant decides the major problems are due to a lack of training, design problems with the supporting IT system, document control problems, and customer input difficulties. These identified issues can be organized into a fishtail cause-and-effect diagram, as shown in Exhibit 28.3. The idea is to identify the potential contributing problems graphically in a way that suggests basic root causes. The consultant can then use the diagram to discuss the problem and its causes with management to obtain some general agreement on the current problem.

Often this type of high-level potential problem cause analysis results in a series of "Have thought about . . . ?" questions that send consultants back for further analysis. However, such an analysis often points consultants toward a recommendation.

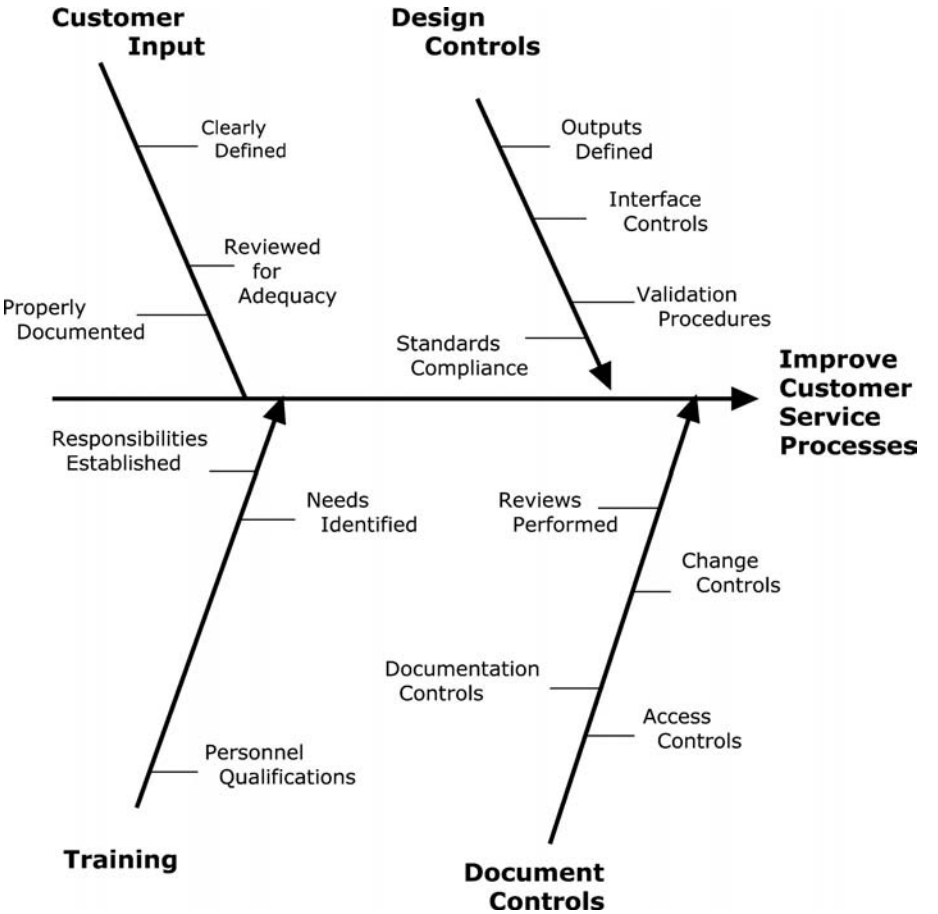


EXHIBIT 28.3 Cause-and-Effect Diagram

(d) Implementing Consulting Recommendations

Consultants should think their recommendations out fairly well, taking into consideration costs and feasibility. Recommendations often are made after more consultative discussions than occur on internal audits. A difference may be that an internal auditor performing a review will go over a draft audit with management to discuss issues surrounding a recommendation. The internal auditor then issues the audit report and expects management responses regarding the corrective action plan.

A consultant making a recommendation often faces a difficult situation. If management agrees to those recommendations, it often asks the same consultant to take an active role in leading their implementation. Most internal auditors have encountered situations where management does nothing in regard to external auditor recommendations; as consultants, internal auditors often must help take the lead role in implementing any recommended actions. This is a significant difference from many internal audit attest activities.

(e) Documenting and Completing the Consulting Engagement

Chapters 16 and 17 discussed documenting internal audit results through formal workpapers and describing them in a formal audit report. Consulting projects have similar but somewhat different requirements. In many instances, the consultant internal auditor may have implemented a new set of desk operating procedures. A major portion of the consulting project consists of procedures that operating personnel can take and use going forward. In other cases, the consulting project should be documented in a manner that management can go forward with the documented results and that the internal audit attest function will be able to fully accept this consulting work if they audit its internal controls.

Perhaps even more than for a traditional internal audit project, with consulting engagements, strong attention should be given to the hours and costs involved. There will often be direct cross-charges, and management may expect to see detailed accounting records supporting those charges. For a normal internal audit project, auditees may receive communications that an audit will be completed after three weeks. When the internal auditors take four or five weeks, auditee management may wonder why it is taking so long but often sees no direct charges for that extended time.

In a consulting internal audit project, management often is asked to absorb the costs of that work. The expansion of a project from the estimated three weeks to an actual five will result in crossover charges to the auditee's ledger, and there must be detailed documentation to support these activities. In addition, to support an adequate separation of duties between internal audit consulting and attest activities, consulting-related projects should be completed in a manner that they always appear to be separate from the internal audit attest review.

28.5 Expanded Internal Audit Services to Management

Consulting represents an expanded and important potential internal audit service to management. Internal audit should offer internal consulting services beyond its regular attest audits. In order to do so, it should present the enterprise with a revised charter and detailed statements describing its consulting capabilities and offerings. Attention must be paid to supporting the independence of these two functions within internal audit. Although an internal audit professional may be working on

one attest project and on consulting projects at another time, these activities must be kept separate and independent, both in fact and in the perception of others.

Properly organized, an internal audit consulting project will provide resources to management in a way quite different from traditional internal audit attest reviews with their often critical internal audit reports focusing on findings and recommended actions. However, if an internal audit function wants to provide internal consulting as an additional offering, this work must be at least as professional as the internal audit attest work. In addition, great care must be given to organizing internal audit consulting activity so that it is not perceived by others as self-serving. That is, internal audit attest findings should not be construed as promotional work to increase consulting projects.

Internal auditors should also have a CBOK understanding of consulting-related standards and of the consulting process. Even if the internal audit function has elected to not engage in internal consulting beyond normal attest work, all internal auditors should understand the role and place of consulting in the overall internal audit process.

Note

1. *International Standards for the Professional Practice of Internal Auditing*, Sections 1130.C1 and C2. These standards are summarized in Chapter 8 and can be found in www.theiia.org.

CHAPTER 29

Continuous Assurance Auditing and XBRL

Continuous assurance auditing (CAA) is the process of installing control-related monitors in information technology (IT) systems such that these monitors will send signals or messages to auditors—usually internal auditors—if the system's processing signals a deviation from an audit limit or parameter. This concept has been around since the early days of IT auditing, when pioneer IT specialist internal auditors developed monitoring tools known as Integrated Test Facilities (ITFs) or System Continuous Audit Review File (SCARF) facilities.[1] These processes date back to the days of mainframe computers. Although those early real-time audit monitor concepts seemed interesting, they were seldom implemented effectively.

The concepts behind ITFs and SCARFs later evolved into today's CAA monitoring techniques but were little used after the 1990s. Today, technology and to some extent the Sarbanes-Oxley Act (SOx) are making CAA a very practicable alternative for auditing automated systems. The testimony of James Castellano, then the chair of the American Institute of Certified Public Accountants (AICPA), during the congressional hearings regarding the fall of Enron emphasizes the importance of using a CAA approach. His February 2002 comments included:

> *The transition to new reporting and auditing models is going to demand not only new audit approaches but personnel of the highest caliber. With this in mind, the profession has been working actively in the following areas:* continuous auditing or continuous assurance *involves reporting on short time frames and can pertain to either reporting on the effectiveness of a system producing data or more frequent reporting on the data itself.*[2] *(Emphasis added.)*

This chapter discusses CAA as an improved alternative approach for reviewing automated systems and what is known as continuous monitoring (CM), business-controlled procedures that can be subject to periodic internal audits. Technology makes continuous auditing approaches much easier to implement, and SOx's potential future requirements for almost real-time financial reporting makes this concept very attractive. CAA calls for installed audit monitors as well as the ability to close an enterprise's financial reports on almost a real-time basis. CAA represents a dramatic change in the audit model, and as CAA becomes more widely accepted, it may change both auditor practices and skill requirements.

Today's enterprises need to retain all forms of operating and historical information, stored on information systems (IS) databases. When these stored data are organized in a series of large, complex, and interrelated databases, this mass of stored data has come to be known as a data warehouse. A data warehouse environment is an almost necessary component for implementing effective CAA processes, as are the tools of data mining and online analytical processing (OLAP). This chapter briefly discusses these concepts and their applicability to internal audit processes.

Finally, this chapter introduces XBRL (eXtensible Business Reporting Language), the AICPA-initiated, extensible business reporting language. XBRL is a standards-based way to communicate business and financial information across multiple enterprises. For example, if enterprises code a standard value on their financial reports in XBRL, such as the total assets or accumulated depreciations, it is very easy to identify that reported financial value despite different physical report formats. XBRL is becoming an increasingly important tool that internal auditors should understand and will almost certainly be using in future years.

Many chapters of this book have highlighted internal audit common body of knowledge (CBOK) areas that we feel should be internal audit requirements. The CAA and XBRL concepts discussed in this chapter are areas where internal auditors need just a general understanding. Internal auditors may not need the skills, for example, to implement CAA processes. However, they should understand that these tools and concepts may be useful in various internal audit processes.

29.1 Implementing Continuous Assurance Auditing

Internal auditing has gone through a series of conceptual changes over time. In its earliest days, auditing was primarily a process of vouching and testing, a concept that goes back to the dictionary definitions of these terms. To *vouch* means to attest, guarantee, or certify something as being true or reliable, and auditors performed tests to support that vouching process. This type of audit process had been used for years. However, as processes became more highly automated, auditors began to rely primarily on reviews of internal controls to support their audit conclusions rather than the old-fashioned vouching. If the controls were adequate and found to be working through tests, there was less need to perform the detailed transaction testing. In this second phase of auditing and through the early 1990s, auditors emphasized reviews of internal controls as the major component of their attest work.

With too many IT applications today and their diverse controls to consider coupled with an ongoing emphasis on increased audit efficiency, auditors—particularly external auditors starting perhaps in the mid-1990s—began to emphasize just higher-risk internal control areas through formal risk analyses. This audit risk analysis process was discussed in Chapter 6 and could be considered a third phase of auditing after, first, "vouch and test," and, second, internal control reviews. Many analyses of what happened after Enron as well as WorldCom, Tyco, HealthSouth, and others raised questions about the audit procedures used. How could all of these failures have happened? Why did the external auditors not see these internal control weaknesses and other problems? One concern often cited was that financial reports, filed with the Securities and Exchange Commission (SEC) and published as annual reports, were unreliable. A second concern and criticism was that the supporting final audited reports were often delivered well after the official statement closing dates

and contained many pro forma, almost best-guess numbers. SOx now requires that financial reports be closed and issued on a much tighter schedule, closer to the enterprise's period ending dates. That SOx requirement calls for continuous-close audits and auditor assurances—what may become the next phase of audit techniques.

(a) What Is a CAA Monitoring Process?

CAA is an audit process that produces audit results simultaneously with, or within a short time after, the occurrence of actual events. Auditor-supervised controls, for example, are installed in a major, enterprise-wide resource application that include alarm monitors and continuous analytical analysis routines to either attest results or highlight items for immediate audit analysis. A CAA is generally independent of the underlying business application with processes that test transactional data against defined control parameters or rules. CAA processes today run automatically on a daily or weekly basis and generate exception reports or alerts for internal auditor follow-up. Similar to the traditional audit process, a CAA is more detective than preventive.

Although the underlying concepts are very similar, sometimes we can confuse continuous assurance auditing and continuous monitoring. The basic characteristics of each are listed next.

Continuous Assurance Auditing

- Repetitive software audit monitors are built into IT applications. For example, if internal audit is interested in financial transactions in some general ledger account above some specified limit, a software change can be installed to monitor any activity that meets the criteria.
- Rather than scheduling periodic internal audits to review an area, CAA records areas of potential interest for internal audit's attention. It is then internal audit's responsibility to follow up on these items.
- Internal audit is generally responsible for the confidentiality of installed CAA software and must adapt to any user-installed IT changes.

Continuous Monitoring

- In many respects, CM is very similar to CAA except that the IT users—often at the direction of management—install CM in an application of interest.
- Rather than looking for individual exception items or unusual transactions, CM often is installed in the form of dashboardlike screens—similar to a gas tank gauge in an automobile—to monitor the ongoing operation and status of the application.
- Internal audit may review CM processes on a periodic basis but often only to gain assurance that the overall process is working.

While the concepts between CM and CAA are similar, their architecture and objectives are different. An internal auditor should have a basic CBOK understanding of the key characteristics of CM and CAA procedures. In its most basic design, a CAA is an independent application that monitors another critical application. Exhibit 29.1 shows a CM monitoring application for an automated payments system. This is a separate parallel set of software that monitors all payment activity by periodic reviews of activity through a payments transaction file. Activity summaries are reported through periodic reports, and any unusual items are highlighted in an

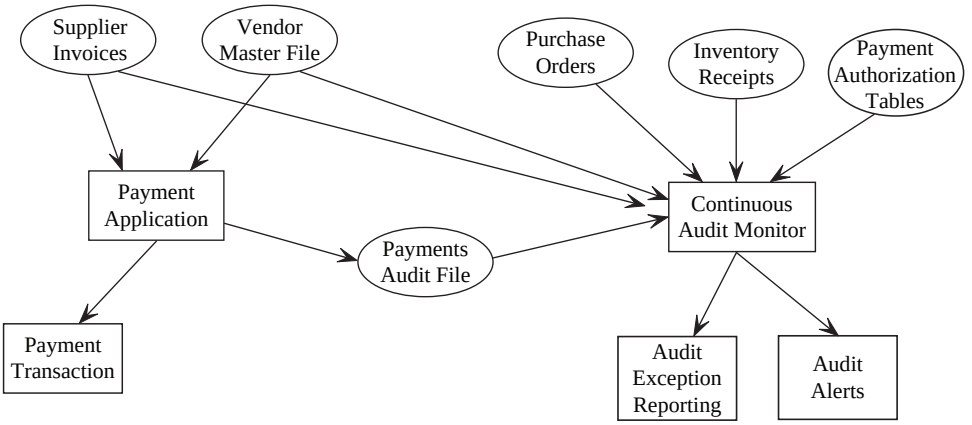


EXHIBIT 29.1 Payment System Continuous Audit Monitor

exception report, probably via an e-mail notice. This type of system is very similar to the kinds of password security monitors in place in many enterprises. Exception activity would be reported on a regular basis, but any red-flag violations would be highlighted for immediate attention.

CAA applications should be more than just monitors that run against application transaction files to highlight exceptions. For many enterprises, IT applications are much more complex. Enterprise resource planning (ERP) systems are an example. These are the all-inclusive application packages, by vendors such as SAP, PeopleSoft, and Lawson, that provide total systems solutions including accounting, general ledger, human resources, and others covering virtually all enterprise applications. These are complex IT systems built around a single or a closely federated set of databases; an average ERP implementation costs some $12 million and takes almost two years to install. Any CAA set of monitors here must be much more complex, as multiple transactions may be updating or depending on multiple database tables. CAA processes are very useful here as they allow monitoring to be installed over the common database structure of an ERP implementation.

Exhibit 29.2 provides a conceptual view of the multiple audit review processes that are elements of CAA. At the base of the exhibit is a stream of measurable, IT application processes such as might occur in a typical complex ERP. The audit team would then identify and establish some metrics it wishes to monitor as well as supporting standards for those metrics. As a simple example, internal audit might be interested in sales division office ERP transactions over $10,000 because management has expressed concern regarding possible unapproved marketing activity. Metrics tools can be built into the ERP processes to monitor all cash transfer transactions with a standard that any amount over this $10,000 limit should be flagged. The process can have multiple levels of metrics and standards with exceptions fed up to a first-level assurance process that would monitor the difference and, in some instances, send a correcting feedback transaction to the ongoing process. The first level of monitoring here might be similar to the warning notes sent to corporate systems users when their mailbox is over 90 percent full.

Other discrepancies would flow up to what the exhibit shows as a second-level monitoring process. This level would produce the reports to management

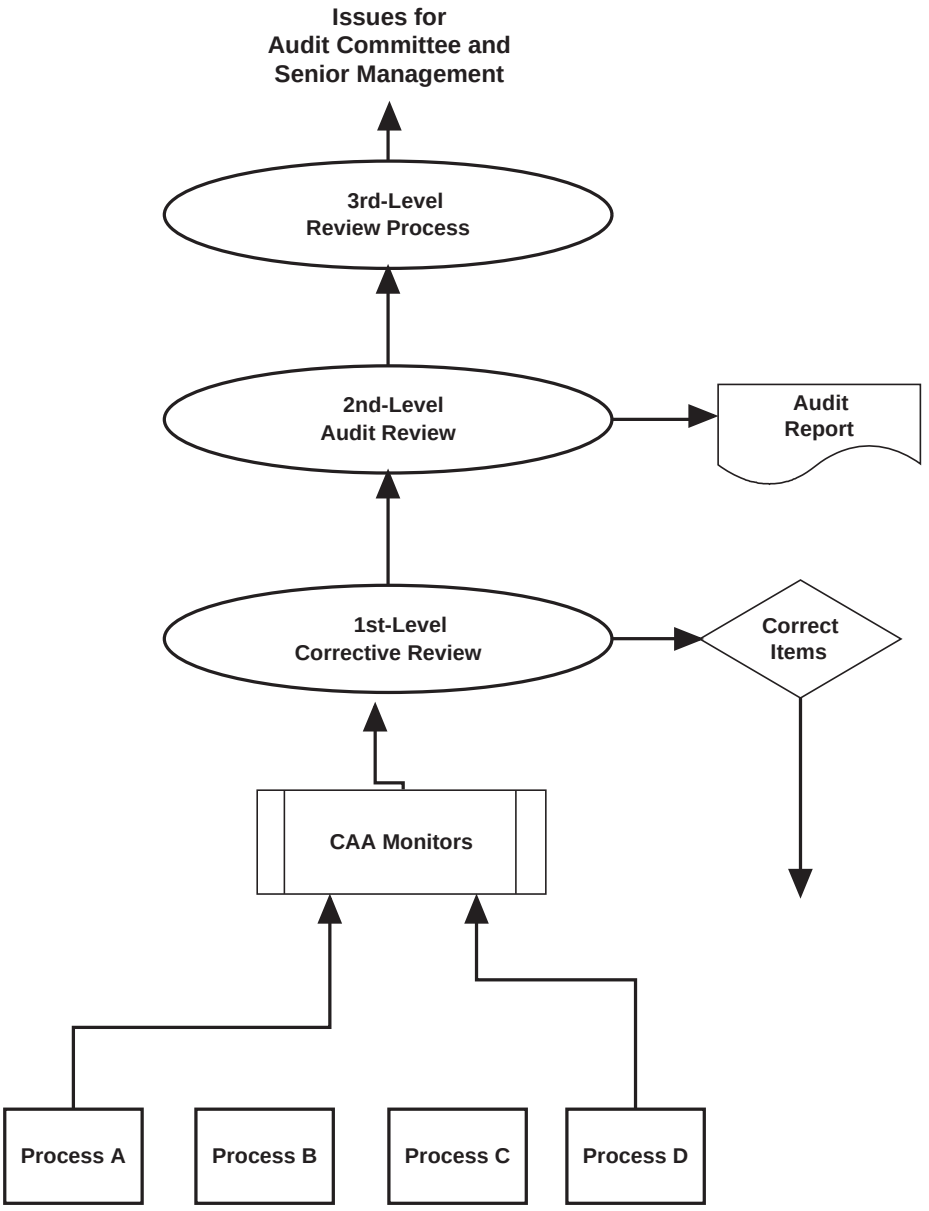


EXHIBIT 29.2 Continuous Assurance Auditing Conceptual Model

or emergency exception notices. Beyond reports, this level could produce more significant audit or assurance actions. In the mailbox-full example, the CAA would initiate a transaction to prevent offending users further access. There is also a third-level CAA review process. Control procedures also can be built into the process to monitor ongoing CAA activity. This is the level that the enterprise can use to report CAA activities to external auditors.

The continuous audit monitoring processes just described can be performed on multiple levels. The first level might be to flag all transactions that pass resources

between the enterprise and some entity of interest, extracting all transactions that match auditor-defined criteria for further analysis, vouching, or reporting. An example might be installing monitors to screen for all financial transactions with some group of countries or companies of interest. A second level would be a bit more sophisticated and would include some limits or logical templates in the evaluation process, such as establishing maximums and minimums in the monitors. On a third and more analytical level, the CAA could examine the formal rules relative to the process monitored. An example here might be the use of system-generated values, such as interest rates or asset returns, and the CAA could perform a comparison of application values with auditor-initiated reasonableness tests using historical values.

At its most basic level, CAA introduces a heightened level of monitoring to application systems. Classic auditor points of control will "disappear" into the processing system, changing recording and measurement tools. The cycle time for making audit-based decisions or actions will decrease greatly as it is based on systems measures. A CAA can create an environment for 24-hour-a-day, 7-day-a-week (24/7) continuous auditing.

A variety of larger enterprises have already implemented CAA processes. The original AT&T, for example, was an early leader, and CAA has become common in the insurance, stock brokerage, and medical claims processing industries. Built around an enterprise's ERP system, CAA is particularly useful for monitoring purchase and payment cycle applications with an emphasis on controls over potential vendor-related fraud. CAA is a valuable tool for any application area where cash is going out the door, such as employee travel accounting, insurance claims, and money-laundering controls.

(b) Resources for Implementing CAA

The concept of launching an audit monitor in an ERP or other business application seems straightforward, but the actual implementation of a CAA in an enterprise often presents challenges. In order to be an independent IT application monitoring process, the CAA should not be installed by the same IT developers who operate the production process. That is, if a CAA has an objective to monitor all marketing expense transactions over X dollars and some certain other conditions, those marketing expense system monitoring controls must be installed independently such that they cannot be bypassed easily. However, installing a CAA process in an ERP or any other business applications often requires strong IT technical skills that may be beyond the capabilities of many internal auditors. Conversely, even if internal audit has the technical skills to install CAA in an enterprise's applications, IT management may look at any such proposal with a high degree of skepticism. IT management often will not trust its internal auditors to install their own CAA monitoring software in production systems environment. If IT agrees to take the CAA software module and test and modify it for production installation, the CAA's independence could be compromised.

This section introduces several vendor-supplied software solutions to install CAA. The products or approaches discussed are not the only ways to install CAA but represent some good starting points.

Good sources for more information CAA can be found at the Rutgers University accounting Web site (http://raw.rutgers.edu/) as well as the Texas A&M University Mays Business School Center for Continuous Auditing (http://business.tamu.edu/cca/). Both are involved with CAA conferences, and papers from past conferences

can be found on their Web sites. The Rutgers site has a wealth of information on CAA approaches and even sponsors conferences on the effective use of CAA. We have selected several CAA implementation examples from these and other sources.

(i) **MICROSOFT'S CAA APPROACH** Microsoft's corporate internal audit function has developed a CAA approach it has called technology enabled continuous auditing (TECA). This internal application serves as a bridge between CAA and CM approaches. TECA has the stated objectives of providing greater risk coverage, increased internal audit productivity, more detailed and frequent testing, and shortened audit cycle times.

We gained an understanding of TECA from a presentation by the Microsoft chief audit executive at the 2008 IIA International Conference. The presentation materials did not provide a complete description of the process, but it appears that Microsoft internal audit is doing an excellent job of implementing an effective internal audit CAA process.

Microsoft internal audit views the TECA application as a transition to continuous monitoring allowing internal audit to analyze transactions as they flow through Microsoft systems and to provide improved internal audit workflow. The TECA implementation at Microsoft shown in Exhibit 29.3 links custom applications, ERP systems, human resource applications, and others. Space does not allow a complete description.

Microsoft internal audit has implemented its TECA system for monitoring travel and entertainment expense reporting, checking for duplicate reported expenses, excessive employee reported out-of-pocket expenses, and inappropriate reported exchange rates. Another area where internal audit is using TECA is for CAA monitoring of SAS No. 99 potential fraud activities (see Chapter 25), where the application

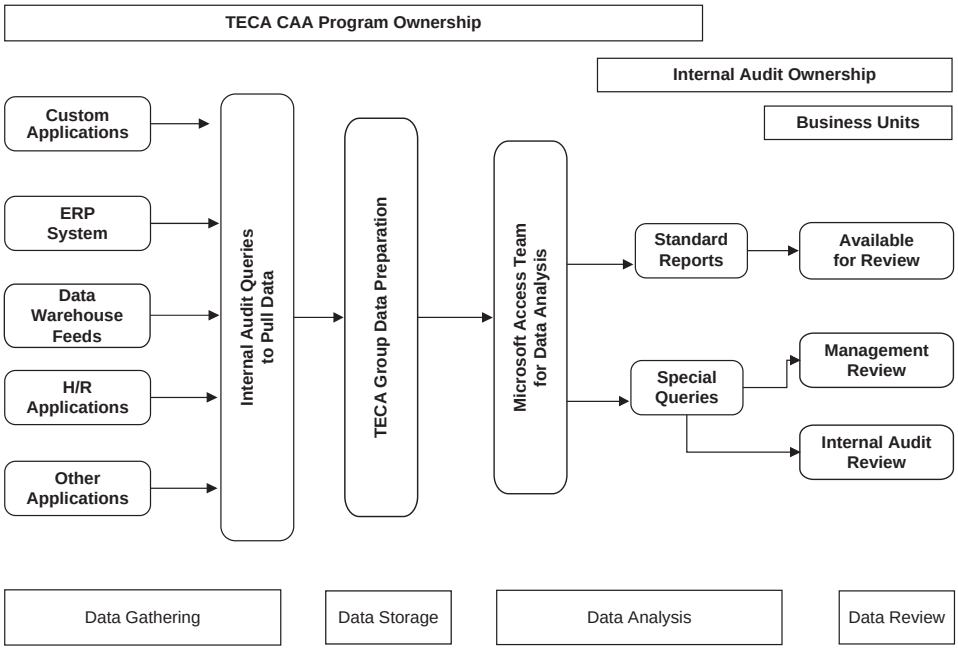


EXHIBIT 29.3 TECA Implementation at Microsoft

identifies potentially inappropriate journal entries posted at month-end as well as large or unusual items for internal audit follow-up.

(ii) ACL CONTINUOUS ASSURANCE SYSTEMS Many auditors have used software products developed by ACL Services, Ltd.,[3] a Canadian-based developer of computer-assisted audit analysis and retrieval software also discussed in Chapter 21. ACL also provides an effective tool for what might be described as first-generation CAA. ACL takes the approach that few organizations today have fully embedded and automated continuous auditing or monitoring applications. Most audit-related testing applications today are simply a series of automated data analysis tests that are manually initiated and run on a regular basis. The ACL approach goes a step further in that the auditor does not need to formally start and run the monitoring program, with the ACL software linked to enterprise files and applications so that it can run in the background. The software is useful for detecting unusual transaction indicators of fraud or identifying duplicate and other overpayments. While not truly continuous audit monitor, ACL suggests the auditors install and run this software based on completion of process steps and periodically. The software then takes a slice of the data, capturing all transactions since the last test process. ACL continuous assurance software is used today by all of the major public accounting firms as well as a large number of major U.S. corporations. An enterprise that is interested in implementing some beginning level of CAA might well consider starting with ACL's assurance product.

(iii) DASHBOARD APPROACH TO MONITORING: BUSINESSOBJECTS AND OTHERS Complex information systems can be built with a wide variety of monitoring programs and displays to allow an operator to review performance and highlight any potential problems. This monitoring approach is similar to the driver of an automobile who faces a dashboard that monitors performance by showing speed, progress by showing miles traveled, status by showing the fuel remaining, and problems by displaying warnings for such items as low oil pressure. This dashboard approach allows the driver to monitor overall progress while the vehicle is in operation and to take action as required. That same dashboard approach can be used with business information systems.

The typical online application of today has a continuous display. In a sales order application, for example, designated users can access the progress of sales recorded, perhaps by product line or region, through an online terminal. However, that monitoring typically covers just one sales application; another screen must be called up to review a related activities handled by other applications, such as ongoing cash collections or returns. Today's ERP applications provide a better environment for such cross-application monitoring as all of the components of the ERP from receiving to general ledger processes are under a common database structure. Several good software products allow enterprises to install dashboard monitors to review overall progress of business transactions and other activities to allow for prompt remedial action when necessary. Two of the better of these software tools are the offerings of BusinessObjects Corporation, a division of SAP, and Cognos Corporation, from Ottawa, Canada. Products from each firm allow an organization to tie a wide variety of diverse applications to a dashboard monitor, enabling users to monitor overall activity.

The console monitors on the old classic mainframe computers acted as a dashboard and monitored all system activity with a constant stream of messages to the

operator. The same concept can be applied to today's ERP applications. They will allow an organization and internal audit to move from an environment of monitored controls to the real-time monitoring of systems operations with adjustments for continuous improvement.

29.2 Benefits of CAA

CAA approaches allow internal audit to deal with IT-based issues on a real-time basis. Rather than waiting for an internal audit that is scheduled only once every year or so, a CAA process provides internal audit and management with an early warning for many areas of internal audit interest. CAA provides internal audit with a tool for proactive risk management. In addition, effective CAA processes should allow internal auditors to develop a better understanding of their enterprise's business environment as well as to support compliance and drive business performance.

By changing traditional internal audit approaches and implementing CAA processes, internal auditors can develop a better understanding of their business environments and the risks to their enterprise. CAA processes can support compliance and provide for the automation of transaction testing for the verification of transaction integrity and validity. CAA creates an environment of continuous testing where internal control failures can be detected and fixed immediately. Although there is some effort involved in implementing CAA, its approach of looking at full populations of data from areas of interest can very much increase the overall effectiveness of internal audit. We are now seeing internal audit functions in major enterprises, such as Microsoft Corporation, adopt CAA approaches. It is a growing future internal audit trend.

29.3 XBRL: Internet-Based Extensible Business Reporting Language

Business today is very much based on Internet-supported applications. The paper-based information reports and the batch systems that once supported them have largely gone away. Virtually all enterprises today are operating in an environment of Internet-supported processes. While a very flexible approach, management and auditors can question Internet-based document integrity. When IT reports were being produced in the classic closed-shop data center, whether on paper or through online systems, there were few questions about the integrity of the reported data, provided that the supporting internal controls were adequate. As long as there were appropriate general and application controls in place, internal auditors had few questions about general data integrity and only had to perform traditional audit tests to acquire a level of assurance regarding the data. However, the free and open nature of the Internet can raise questions about the integrity of transmitted data. How does the user know that the file of data transmitted through the Web is actually what it is represented to be?

Coding or reporting languages solve some of those concerns, and XBRL, an industry standard approach for the publishing, exchange, and analysis of financial and business reports and data, offers an excellent solution. XBRL is an open-standard business reporting language developed by a consortium of over 200 companies and agencies, and strongly supported by the AICPA in the United States. Delivering benefits to investors, accountants, regulators, executives, business and financial analysts, and information providers, XBRL is rapidly becoming a worldwide standard that

provides for the publication, exchange, and analysis of complex financial information in corporate business reports in the dynamic and interactive realm of the Internet. XBRL provides a common format for critical business reporting processes, simplifying the flow of financial statements, performance reports, accounting records, and other financial information between software programs. XBRL defines a consistent format for identifying data and for business reporting to streamline the preparation and dissemination of financial data and to allow analysts, regulators, and investors to review and interpret the data. As a result, XBRL can save time and money when information consumers within and outside of a company analyze complex operations and financial data. In the post-Enron era of SOx, XBRL is an important tool for providing consistent business and financial reporting.

(a) XBRL Defined

XBRL is an Internet standard, just as HTML is an Internet standard for browsing, MP3 is the standard for digital music, and XML (e*X*tensible *M*arking *L*anguage) is the standard for electronic commerce. XBRL uses standard Internet XML data tags to describe financial information for public and private companies and other enterprises. Its controlling group, XBRL International, is a professional affiliation of more than 200 enterprises as well as governmental jurisdictions that collaboratively produce standard specifications and taxonomies that anyone can license royalty-free for use in their applications. Just as we have established formats for Internet e-mail addresses or Web access links, XBRL provides both a standard description and classification system for the contents of accounting reports. Data can be taken from an accounting information system and XBRL coded to produce an electronic annual report including all financial statements, the auditors' report, and Form 10K notes. The document can then be read directly by computer programs or end users or, more likely, coupled with a style sheet to produce a printed annual report, user-friendly Web pages or an Adobe Acrobat™ file. Similarly, internal business reports and regulatory filings can be output in a variety of forms.

The Web is filled with many positive comments about XBRL; perhaps the most frequently quoted comment is: "XBRL is . . . perhaps the most revolutionary change in financial reporting since the first general ledger."[4] XBRL provides a method for enterprises to report their financial information in a format that can be easily read and understood by others. It allows for efficient data collection and publishing as well as serving as a tool for improved data validation and analysis. Exhibit 29.4 illustrates how XBRL can improve the transfer of data and information across systems and entities. As the exhibit shows, financial data from an enterprise's ERP, general ledger, and other financial systems can be all coded in XRBL. That coded information can then be used, either currently or in the future, for reports to banks, annual reports, SEC EDGAR[5] filings, and others. XBRL is a consistent approach for reporting to investors, credit agencies, and governmental units.

(b) Implementing XBRL

XBRL is an evolving standard. Visionaries have praised the concept, tools and standards have been established, and there have been some—but not many— early adopters. For example, Microsoft Corporation has been filing its SEC Form 10K report in XBRL format since 2002, and General Electric is using it for its internal

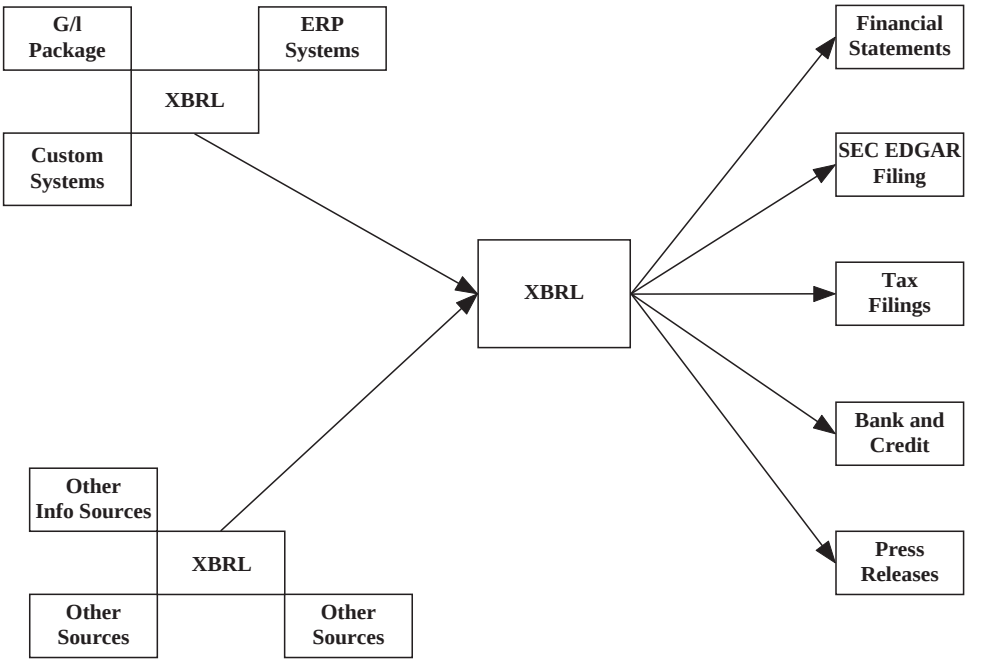


EXHIBIT 29.4 XBRL Interoperability Uses

company reporting. Governmental regulators have seen the value of financial reports issued in a consistent and traceable format, and the U.S. Federal Deposit Insurance Corporation now requires that federal bank status call reports be submitted in XBRL format. The standard can save on costs and provide reporting flexibility by eliminating proprietary accounting system dump formats and doing away with manual copy-and-paste consolidation and reporting. We will probably see SEC requirements for the use of XBRL over the upcoming years. More significantly in the United States, the SEC is converting its EDGAR financial information database to XBRL and is moving to making XBRL a mandatory requirement for financial report filings.

As an Internet business reporting language for financial data, XBRL is similar to HTML for browsers, where the Internet user clicks on some tagged reference to get pointed to another site. Under XBRL, Internet financial data are tagged in a way that they can be recognized and properly interpreted by others using applications based on a standardized XBRL vocabulary of terms, called a taxonomy, to map results into agreed-on categories. An example of this XBRL taxonomy is the markups or coding for well-defined concepts within the current U.S. generally accepted accounting principles (GAAP) including "accounts receivable trade" or "allowance for doubtful accounts." No matter where it is located in the report format, a value can be recognized as the "allowance for doubtful accounts" whether within one enterprise's reports or across multiple enterprises. However, GAAP may vary somewhat depending on whether the enterprise is a retailer, a minerals extraction mining company, or any of many other variations. XBRL qualifiers set these categories. A major saving with XBRL is the reduction of the data manipulation required when an enterprise needs to reposition the output from its financial systems to meet the needs of diverse users. A quarterly Internal Revenue Service tax form is very different in format and

content from the format in a quarterly SEC filing, although the information needed to file both documents typically comes from the same financial database. With XBRL, information will need to be entered only once; the same information can be rendered as a printed financial statement, an HTML document for a Web site, an EDGAR SEC file, a raw XML file, or a specialized reporting format, such as periodic banking and other regulatory reports.

Paperless reporting is facilitated here as well. Prior to XBRL, it was necessary to extract financial information for reports from databases such as a general ledger, then process that extracted information multiple times depending on the needs of the user. For example, a typical balance sheet would need to be individually processed for SEC filings, for placement in the annual report, for examination by external auditors, and for analysis by management. Each process could require an extra handling of the information to create the desired report. With XBRL, the information is coded once and is then ready for extraction electronically into reports for all information users. With the proper tools in place, the desired output for all uses of the balance sheet information can be transmitted electronically, without the need for paper-based reports. There is only one authorized version of that balance sheet with its data appearing in other reports or sources where needed.

Although its use is limited today, XBRL is quickly becoming the standard. Whether mandated by a regulatory reporting agency such as the SEC, launched by visionaries in the enterprise, or just because everyone else is using XBRL to code their financial reports, most enterprises will soon be using it as part of their financial reporting procedures. If there currently has been no action, an internal auditor should have conversations with appropriate persons in IT as well as financial management to determine their plans for XBRL implementations. As a first step, however, the interested internal auditor should gain a high-level CBOK understanding about XBRL. Since it is an XML-based, royalty-free, and open standard, much information is available through the official Web site (www.xbrl.org). That site will point interested persons to a wide variety of papers, presentation sets, and descriptions of its use.

Because it is still an evolving technology, there are some risks of error here. An enterprise needs to select an appropriate taxonomy and appropriately tag its data. Going back to our earlier example, there will be one taxonomy for a manufacturing and distribution firm and another for a petroleum refinery. Starting with the wrong taxonomy will cause multiple control problems. Once an appropriate taxonomy is selected, procedures need to be in place to ensure that the tagging of data is complete and accurate. This is the same type of control concern that Internet browser users occasionally encounter when clicking on a link and getting pointed to the wrong or a nonexistent site. It is frustrating when surfing through the Web, but potentially could cause greater problems when retrieving or reporting financial data. Internal audit should review procedures to ensure that controls are in place for that XBRL data tagging. Even though these kinds of endeavors often start as a pet project by some member of the IT group, that tagging should be documented in a controlled environment.

XBRL is rapidly becoming a new rule standard for Web-based financial reporting and supporting systems in the United States, the European Union, and throughout the world. As this edition goes to publication, many have predicted it will become the SEC reporting standard by 2010. As John Connors, chief financial officer of Microsoft, stated in 2002 on releasing his company's financials in XRBL: "We see XRBL as not only the future standard for publishing, delivery and use of financial information over the web, but also as a logical business choice."[6]

29.4 Data Warehouses, Data Mining, and OLAP

For many years, data storage was considered a rather mundane component of the IS infrastructure. Back in the mainframe computer days, data necessary for immediate short-term access was stored on mass storage disk drives with other less essential data copied to magnetic tape drives. However, those old rules have not worked that well today as applications have grown larger and more complex and as users became ever more hungry to analyze and understand that protected data. Data storage has now become a major component of the IS enterprise.

This section briefly introduces several important storage management practices and concepts, but space limitations as well as the breadth of the topic restrict our discussion of storage management. Internal auditors, however, should develop an understanding of this increasingly important IT component. Storage management control procedures are an important part of IT general controls, as discussed in Chapter 18, but were too often ignored in past discussions of IT controls.

(a) Importance of Storage Tools

Computer equipment manufacturers have been experimenting and introducing new storage devices over the years. In the mainframe, legacy-systems world, the emphasis was always on trying to pack more data storage capacity on a reliable disk drive. During the 1970s, storage techniques ranged from the use of large rotating drum devices to experiments with holographic storage. Rotating disk devices and magnetic tape prevailed, and mainframe computer operations centers in the 1980s devoted large amounts of floor space to these storage devices. During that same period, an increasing amount of storage resided on desktop computers with their own very reliable and increasingly high capacity C drive hard disks. Systems and databases were getting larger, and there was a need for a reliable tool to handle these larger storage needs. The storage world really changed when EMC Corporation[7] launched a product called a Symmetrix, the size of a kitchen refrigerator, that was a massive array of several hundred very high speed hard disk devices managed through a series of controller devices and attached to each other and connecting computers through extremely fast and reliable fiber channel connections. Soon other competitors launched similar storage management tools, capabilities increased, and storage costs dropped dramatically. Storage management as a separate technical profession was launched.

Many enterprises experimented with these new storage device offerings, adapting them to meet user demands for more and more storage capacity. This led to storage management arrangements in data centers called "just bunches of disks" (JBOD) configurations, with these storage devices all connected to servers or central computer systems. A concept called network attached storage (NAS) soon evolved; here the storage devices were connected to a network to provide file-level access to the stored data. Specialized NAS servers were added to allow applications to determine the locations of stored data such that anyone on the NAS could access stored data, and additional capacity could be added easily. From NAS, we have moved to storage area networks (SANs), where all storage devices are installed in a configuration similar to the local area network of office desktop computer systems. With SANs, stored data can be spread across multiple devices with easy switching from one to another.

Technology moves forward, and today we have content addressed storage (CAS), which moves storage from being just an archive to an environment that can more easily respond to direct user and application requests in formats ranging from classic database formats to digital photos. In addition, we are increasingly using the concept of storage virtualization, where that actual physical location of the storage is replaced by abstract logical references. In essence, storage management is an increasingly important component of an enterprise's IT environment. Internal auditors can provide a major service to management by reviewing storage management capabilities including device utilization, performance, and traffic patterns. Storage management problems can limit systems availability and present difficulties in meeting service-level agreements.

(b) Data Warehouses and Data Mining

Recently, the concept of data warehousing has evolved into a unique and separate business application class. An internal auditor may ask, "What is a data warehouse?" A simple answer is that a data warehouse is managed data situated outside of the operational IT facility. The primary concept of data warehousing is that the data stored for business analysis can be accessed most effectively by separating it from the operational systems. Many of the reasons for this separation have evolved over the years. In the past, mainframe legacy systems archived inactive data onto tapes, and many analysis reports ran from these tapes to minimize the performance impact on the operational systems. Advances in technology and changes in the nature of business have made many of these business analysis processes much more complex. Today data warehousing systems support the OLAP systems to be discussed.

Data warehousing systems are most successful when data can be combined, in the true concept of a central warehouse, from multiple operational systems at a place independent of the source applications. The data warehouse can combine data from multiple applications, such as sales, marketing, and production systems. Many large data warehouse architectures allow for the source applications to be integrated into the warehouse incrementally. This allows for cross-referencing and time-dimension data filtering, allowing an analyst to generate queries for a given week, month, quarter, or a year or to analyze data from the old and the new applications.

Building a data warehouse can be a complex task. Data must be gathered from multiple sources, scrubbed to clean up problems, and then converted or transformed to the data warehouse databases. Exhibit 29.5 shows this general concept at a very high level, where an enterprise has separate systems for its order processing, product management, and marketing. The key information elements here will be transformed to a consistent data warehouse format, existing backups will be converted, and, going forward, these systems will feed the data warehouse on a regular basis. The idea is not necessarily to move all application operations to the data warehouse repository but to convert from their separate applications for future analysis. The data warehouse concept can be compared to a department of accounting analysts where each employee downloads some data to his or her desktop system and produces separate analysis reports. In a warehouse type of environment, all of the separate data might be combined to one server such that all analysts can combine and share the data.

An objective of a data warehouse should be to make information retrieval and analysis from that facility as flexible and as open as possible. Low-end tools, such as

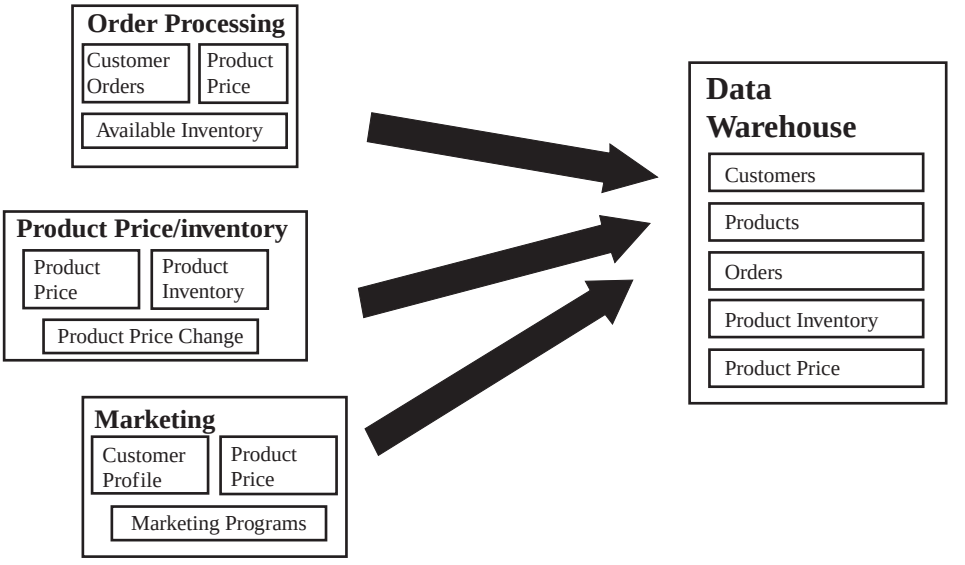


EXHIBIT 29.5 Data Warehouse Transformation Example

simple query capabilities, may be adequate for users who need only to reference the data warehouse quickly; other users may require powerful multidimensional analysis tools. Data warehouse software analysis tools should be implemented to assist in this query process. Many software retrieval tools are available, and after becoming familiar with a low-level data warehouse tool, users may be able to justify the cost and effort involved with using a more complex tool. Internal auditors should be aware of the processes in place and the controls to limit access to authorized users. Because of the massive amount of historical data contained in a data warehouse, a high level of security and privacy tools are needed.

Many reports that are generated from a data warehouse facility will be just canned reports showing warehouse summary data. They may be produced regularly or on request. In other instances, users may perform specific queries against the data warehouse accumulated summary data. The real strength of the data warehouse is its ability to allow analysts to perform *data mining*. This is an evolving software retrieval technique, where users start with summary data and drill down into the detail data looking for arguments to prove or disprove a hypothesis. The tools for data mining are evolving rapidly to satisfy the need to understand the behavior of business units, such as customers and products. Even though data mining may account for a very small percentage of data warehouse activity, it is the key strength of the data warehouse for most enterprises. The reports and queries of the data warehouse summary tables are adequate to answer many "what" questions, but the mining-like drill down into the detail data provides answers to "why" and "how" questions.

A data warehouse can be a better single and consistent source for many kinds of data than the operational systems. However, because most information will not be carried over to the data warehouse, it cannot be a source of all system interfaces. Internal auditors should have a CBOK general understanding of the concept of data warehousing. Internal auditors seeking more information should do a Web search on the topic.

(c) Online Analytical Processing

Online analytical processing (OLAP) is a basic data analysis process for a range of essential business applications, including sales and marketing analysis, planning, budgeting, statutory consolidation, profitability analysis, balanced scorecard, performance measurement, and data warehouse reporting. Although OLAP is neither a new nor an obscure concept, it is not widely understood by many managers, internal auditors, and even IT professionals. OLAP is a category of retrieval software that enables analysts to gain insights into data through a wide variety of different views and dimensions of information that has been transformed from raw data. The challenge for many enterprises faced with a mass of data is the need to better understand any related trends. Consider the questions and concerns at a large enterprise selling multiple product lines from various facilities. Which product lines are the most profitable? In which area or markets are sales increasing or declining? Do customer return patterns represent any overall trends? Answers to these and more are the functions of OLAP.

OLAP is the dynamic multidimensional analysis of consolidated enterprise data supporting end user analytical and navigational data. One way of thinking about OLAP concepts is to consider the model of a very complex, very large spreadsheet. We normally think of spreadsheets primarily as two-dimensional arrays of rows and columns where we can do searches, calculations, and types of analysis across these rows and columns as well as over multiple two-dimensional pages. However, sometimes data are too complex or there are just too much to place in an Excel-type spreadsheet. OLAP software offers these features:

- **Multidimensional conceptual views.** Calculations and modeling applied across multiple dimensions, through hierarchies and/or across members. Software tools here may allow analysis across 8 to 10 or more dimensions.
- **Trend analysis over sequential time periods.** Beyond frequent multidimensional needs for looking at data, OLAP tools can consider any data item in terms of sequential time period trends.
- **Drill-down capabilities to deeper levels of consolidation.** Using OLAP, the user can highlight a data element and then easily drill down to examine the basic data that created the item of interest.
- **Intuitive data manipulation.** OLAP tools have the ability to allow "if A, does this imply B?" types of data manipulation.
- **Rotation to new-dimensional comparisons in the viewing area.** OLAP allows a user to flip a complex database on its side and examine all of the data from that different perspective.
- **Reach-through to underlying detail data**. OLAP users can better see the data trends that supported some conclusion.

These are some of the major attributes of an OLAP application. Enterprises typically implement OLAP in a multiuser client/server mode with the objective of offering users rapid responses to queries, regardless of database size and complexity. OLAP helps users synthesize enterprise information through comparative, personalized viewing as well as through analysis of historical and projected data in various "what-if" data model scenarios.

A variety of software products perform OLAP functions, but all comply with a basic set of features first defined by the prominent software engineer E. F. Codd.[8] The general characteristics of an OLAP application, just described, are part of Codd's general model and should be part of any installed OLAP application installed in the enterprise.

OLAP is not necessary for every enterprise. Some enterprises may not have the large amount of diverse data for which OLAP procedures will be cost beneficial. Selecting the right OLAP product is difficult but very important, if projects are not to fail. If an enterprise is considering the purchase of an OLAP product, internal audit should review the control procedures for the new software. If the enterprise is using OLAP software, internal audit should become familiar with it. Although we have talked about OLAP as a useful analytical tool for general business purposes, it also is very useful for extensive audit queries over data.

29.5 Newer Technologies, the Continuous Close, and Internal Audit

This chapter has introduced some important newer and evolving internal audit approaches and technologies. Storage management represents a field of growing importance to the enterprise and its IT resources. CAA concepts are becoming increasingly common as an internal audit tool, and all internal auditors should have, at least, a CBOK general understanding of the concept and where it might be practicable in their own enterprise.

Enterprises may be required to use the XBRL format in financial report filings as this book is released for publication. While it is much more of a convenience tool, such as using HTML notation as opposed to plain text for Internet communications, XBRL will soon become a standard protocol for many forms of financial reporting. This is another important concept where internal auditors should have a CBOK understanding.

SOx rules, as discussed in Chapter 4, require all registered enterprises to close their books for periodic financial reporting on tighter and tighter schedules. External auditors performing those reviews as well as management are requesting timely internal control assessments of those supporting systems. This fact points to the growing importance of the continuous assurance auditing techniques discussed in this chapter. As these time requirements get tighter, management will demand tools to help close the books and produce financial reports even more promptly. The ultimate result will be the continuous close, where the summarized results at the end of a business day represent the overall results for the enterprise up through the end of that business day. Many enterprises are already experimenting with these approaches, and the SOx regulatory requirements as well as today's technology capabilities will continue to point enterprises in that direction. This continuous-close direction will point to new opportunities and internal controls concerns for internal auditors.

While there have always been data storage concerns, going back to the days of punched cards, the needs for accurate and efficient storage processes are increasing. Internal auditors whose reviews of IT controls have been limited to computer hardware and network general control issues should begin to devote more attention to storage management. This chapter has also introduced several data storage

concepts, such as data warehousing and OLAP, but at a very high level. Internal auditors should be aware of these trends and their internal control implications as they are installed in more and more enterprises.

Notes

1. Robert Moeller, *Computer Audit, Control, and Security* (New York: John Wiley & Sons, 1989), discussed how internal auditors can build ITF and SCARF facilities.
2. http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/Archive+-+Schedule+for+Congressional+Hearings+on+Enron+Situation.htm.
3. ACL Services, Ltd., 1550 Alberni Street, Vancouver, British Columbia V6G 1A5, Canada.
4. Ernst & Young, LLP, "What Is Web Enabled Business Reporting?" Ernst & Young LLP; www.ey.com/global/content.nsf/International/XBRLWeb_Enabled_Business_Reporting.
5. An acronym whose meaning really does not matter today, EDGAR is the SEC's forms and filing database; it can be found at www.sec.gov.edgar.
6. Microsoft PressPass, "Microsoft Becomes First Technology Company to Report Financials in XBRL," March 5, 2002, Microsoft.com.
7. EMC Corporation, Hopkinton, MA. The author of this book worked at EMC in the past and helped to launch their Operations Management Consulting group.
8. For background, Codd (1923–2003) was the inventor of the relational database model now used in many if not most IT databases, including the Oracle and IBM's DB2 database products.

PART VIII

Internal Auditing Professional Convergence CBOK Requirements

CHAPTER 30

ISO 27001, ISO 9000, and Other International Standards

In the years following World War II, the United States became the worldwide economic and political leader. This dominance was so great that many in the United States all but ignored some commercial best practice standards set elsewhere in our increasingly globally connected worldwide economy. However, these best practice standards and processes are often collaborative efforts that take into account worldwide national needs and requirements. The international standards of the International Organization for Standardization (ISO; www.iso.org),[1] based in Geneva, Switzerland, cover a wide range of areas, ranging from defining fastener screw threads in an automobile engine, to the thickness of a personal credit card, and to information technology (IT) quality standards. These standards have also been expanded over the years to cover many areas that are important for enterprise governance and quality.

Internal auditors need to have a greater understanding of the role of these ISO standards in an enterprise today. The management and implementation of many ISO standards usually brings an internal auditor out of the corporate office and to enterprise production areas. Quality auditors, whose background and approach often are quite different from Institute of Internal Auditors (IIA) internal audit teams, play an important role here. While Chapter 31 discusses the role of quality auditors who follow the standards set by the American Society for Quality (ASQ) professional organization, all internal auditors should have a common body of knowledge (CBOK) general understanding of ISO standards and their use in enterprises today.

This chapter provides an overview and introduction to several of the many ISO standards that are particularly important for internal auditors. The focus is on ISO 9001 quality standards and ISO 27001 computer security standards. The chapter also introduces several other ISO standards, including international standards for IT management systems and for quality management. Enterprise compliance with appropriate ISO standards is important worldwide today, as they establish benchmarks for worldwide compliance. That is, if an enterprise follows some ISO standard and if its compliance to the standard is accredited by a recognized outsider reviewer, the enterprise's compliance to the standards will be recognized worldwide.

30.1 Importance of ISO Standards in Today's Global World

The ISO is responsible for developing and publishing a wide range of international standards in many business and process areas. Some of these standards are very broad, such as ISO 14001, which covers effective environmental control systems, while others are very detailed and precise, such as a standard covering the size and thickness of a plastic credit card. The broad ISO standards are important because they allow all worldwide enterprises to talk the same language when they can claim that they have, for example, an effective ISO 14001 environmental control system. The detailed ones are also very critical to allow, for example, an ATM machine anywhere in the world to receive the same size and thickness of a credit card.

ISO standards are developed through the collaborative efforts of many national standards-setting organizations, such as the American National Standards Institute and similar groups throughout the world. The process begins with a generally recognized need for a standard in some area. An example would be ISO 27001, which outlines the high-level requirements for an effective information security (IS) management system. The ISO 27001 standard was developed through the efforts of international technical committees sponsored by ISO in cooperation with the International Electrotechnical Commission international standards-setting group. The standard is not specific in its detailed requirements but contains many high-level statements along the lines of "the organization shall. . . ."

Because numerous international governmental authorities, professional groups, and individual experts are involved in the standard-setting process, building an ISO document typically is long and slow. An expert committee develops an initial draft standard covering some area, the draft is sent out for review and comments with a specified due date, and the committee then goes back to review draft comments before either issuing the new standard or sending a revised draft out for yet another round of review and suggested changes. After many drafts and comment periods, the standard is published. Enterprises can then take the necessary steps to comply with the standard. To certify their compliance, they must contract with a certified outside auditor, with skills in that particular standard, to attest to their compliance.

Many U.S. enterprises first got involved with these international standards through the launch of ISO 9000 quality management system standards in the 1980s. At that time, many U.S. companies were faced with high-quality design standards found in many foreign products, such as Japanese automobiles. Japanese enterprises had designed many high-quality products following what became ISO 9000, and U.S. manufacturers began to step up to the plate by modifying their own processes to comply with these higher standards of product quality. Compliance with the ISO 9000 standard allowed worldwide enterprises to design their operations in accordance with a single, consistent standard and then to assert that they have a quality management system in place in accordance with the international standard.

ISO standards are much more controlled than the Information Technology Infrastructure Library (ITIL) best practices guidelines discussed in Chapter 18. The standards are published and controlled by the ISO organization in Geneva following strict copyright rules. They cannot be downloaded through a casual Google search but must be purchased. Many of the ISO standards are just very detailed outlines of practices to be followed. While certainly out of context, Exhibit 30.1 is an extract from a small section of the ISO 27001 IS management systems standard on the control of documents for an information security management system (ISMS). With

EXHIBIT 30.1 ISO Standards Example: 27001 on Management Commitment

5 Management Responsibility

Management Commitment

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

a. establishing an ISMS policy;
b. establishing roles and responsibilities for information security;
c. ensuring roles and responsibilities for information security;
d. communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;
e. providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMA (see 5.2.1);
f. deciding the criteria for accepting risks and the acceptable levels of risk;
g. enduring that internal ISMS audit are conducted (see 6); and
h. conducting management reviews of the ISMS (see 7).

Source: The terms and definitions taken from ISO/IEC 27001:2005 Information technology security techniques—Information security management systems—Requirements clause 5.1 a through h, are reproduced with permission of the International Organization for Standardization (ISO). This technical report can be obtained from any ISO member and from the Web site of the ISO Central Secretariat at www.iso.org. Copyright remains with ISO.

some references to other sections of this standard, the guidance is clear, unambiguous and often points to other areas for follow-up. For example, but not included in this exhibit for brevity, line 5b states that management should establish roles and responsibilities for information security. In other words, it is a prompt for appropriate levels of action. Taken together, the items could also become checklist questions for internal auditor reviews.

If it so chooses, an enterprise can follow and rely on ISO standards similar to the ITIL best practices discussed in Chapter 18, but ISO standards usually represent much more than just best practices. They represent performance measures for an enterprise and its peers. By adhering to these worldwide standards, an enterprise can show that it is operating in accordance with a consistent international standard. ISO 13485 on quality management regulatory requirements for medical devices, for example, defines the quality standards covering human healthcare devices. The standard calls for an enterprise manufacturing such devices to establish appropriate calibration controls. Because of the different calibration approaches worldwide, the standard does not specify just one approach; it merely requires that enterprises have appropriate mechanisms in place.

As mentioned, not only does an enterprise have to change its processes to comply with an ISO standard, but it must demonstrate such compliance to others. In order to attest to such compliance to an ISO standard, an enterprise must contract with an authorized outside reviewer to assess its adherence to that standard. This ISO certification is a process similar to an external audit of financial records performed by certified public accountants (CPAs). Financial statement audits require a licensed CPA external auditor to assess whether an enterprise's financial reports are "fairly stated" following good internal controls and recognized accounting standards. These are high-level words, but when either an investor or the Securities and Exchange Commission (SEC) finds such a signed external audit report along with the final

reported results, there is a level of assurance that these financial reports are fairly stated and are based on good internal control procedures.

The ISO certification process also is similar to a CPA-led financial audit based on the auditee's compliance with generally accepted auditing standards (GAAS) performed by a major public accounting firm. No "Big 4" set of major ISO auditing firms exists, but national standards-setting organizations qualify outside reviewers to perform external audits of various ISO standards. There is no ISO GAAS, however, but a wide degree of diversity in audit objectives, since a reviewer for ISO 27001 on IT security management systems will be looking for different control procedures than would a reviewer for ISO 13485 medical device quality management systems. In all cases, however, the qualified ISO outside auditor may identify areas for corrective actions and publish a report to management similar to an internal audit process. Once the ISO auditor's recommendations have been corrected, the outside reviewer will certify that the enterprise is in compliance with that standard.

Once certified, the enterprise can advertise to the outside world that it has an effective process in place that meets a specific ISO standard. For example, a customer would want to know if a potential supplier of a medical diagnostic device is in compliance with ISO 13485. That same medical device manufacturer would want to gain assurance that its prime component suppliers are similarly ISO qualified.

30.2 ISO Standards Overview

Although virtually all publicly traded enterprises must have audited financial statements, compliance with appropriate ISO standards is not mandated. Because of SEC financial reporting rules, the lack of an audited financial report or a report with an unfavorable auditor's opinion can be very damaging for a publicly traded enterprise. In most instances, compliance with an ISO standard is only voluntary but often it is essential. Regarding the ISO standard covering the thickness and size of a personal credit card, an enterprise that issued cards or card readers that were not in compliance with the standard would fail in the marketplace.

ISO standards covering quality management systems are a bit different. An enterprise can all but ignore a standard such as ISO 9000 calling for a quality management process and still succeed within a national marketplace. For example, in the United States, some senior managers have looked at this ISO standard as "too much paperwork" and have made only minimal efforts to achieve compliance. However, as we move to a more worldwide business trading environment, many more enterprises with global operations will request such a certification. What was once just nice to have has become almost mandatory.

Internal auditors should attempt to learn more about the status of the ISO quality systems standards compliance process within their enterprise. Some standards, such as the thread pattern on a bolt or the thickness of a credit card, will have to become mandatory if the enterprise seeks worldwide sales. Quality standards, as shown in Exhibit 30.1, require that improved processes be established and monitored. If a company has a separate quality audit function, as described in Chapter 31, or an engineering function, internal audit should learn about levels of activity and compliance with appropriate ISO quality standards. Although there is a wide range of ISO standards, the next sections discuss several that are important in today's world of heightened internal controls and governance.

(a) ISO 9001 Quality Management Systems and Sarbanes-Oxley

As mentioned, ISO 9000 has a heritage dating back to World War II, when both sides of the conflict required strong product uniformity while operating at high levels of production volume. Even if the products produced were bullets and bombs, there was a need for strict product quality control. The results on the Western Allies' side were some strong quality assurance standard procedures and the emergence of industrial engineers–production quality assurance and quality control specialists. After the war, ISO was established as part of the General Agreement on Trade and Tariffs, one of the international agreements to bring the world to more of a peacetime environment. ISO 9000 on quality management systems was one of the earlier ISO standards. It first received most attention in the newly recovering European countries.

Japan, another country that was another rebuilding and recovering after the war, strongly embraced quality management systems in the 1950s and 1960s. The country really got started by inviting a series of U.S.-based quality systems experts, such as W. Edwards Deming and others, to help. In many instances, these experts were all but ignored in the United States. However, their philosophies and techniques were heavily embraced by Japanese industry, and by the mid-1970s, Japanese electronic and automobile manufacturers began to make deep inroads into U.S. markets due to the quality and value of their products. Despite the U.S. manufacturers' dominant product offerings and market advantages, many began to recognize that the Japanese-manufactured products were superior in many respects to their own. ISO 9000 quality standards became an increasingly important factor in measuring and assessing the quality of products.

ISO 9000 is an important family of standards for quality management systems. Maintained by ISO, these standards include requirements for such matters as:

- Monitoring processes to ensure they are effective
- Keeping adequate records
- Checking output for defects, with appropriate corrective action where necessary
- Regularly reviewing individual processes and the quality system itself for effectiveness
- Facilitating continual improvement

Each of these points refers to processes, not specific actions. However, for enterprises to assert that they are in compliance with ISO 9000 (actually 9001), for example, often they must make significant changes to their management procedures and supporting documentation. Compliance with an ISO standard also creates a required level of expectation. Any enterprise that holds itself to such standards is stating that it has effective quality systems in place. A company or enterprise that has been independently audited and certified to be in conformance with ISO 9001, for example, may publicly state that it is "ISO 9001 certified" or "ISO 9001 registered." Certification to an ISO 9000 standard does not guarantee the compliance (and therefore the quality) of end products and services; rather, it certifies that consistent business and production processes are being applied.

The actual certification is achieved through a review by a registered audit expert certified for the particular ISO standard. As discussed, this process is similar to the CPA's review and certified audit of an enterprise's financial statements. Regulated

by their national standards organizations, these auditors are authorized to register an enterprise's compliance with an ISO standard.

(i) ISO 9000 DOCUMENTATION PROCESSES ISO 9000 and other ISO standards impose heavy documentation requirements on an enterprise. It is not sufficient for an enterprise just to claim that some process has been documented once. There must be an ongoing process to keep that documentation current over time. In past years, many enterprises created documentation but did not keep it current. This is similar to the situation that many internal auditors often face. Internal auditors would ask if some system or process they were reviewing was documented. Often they were told that the documentation was out of date or nonexistent. This lack of documentation would then become an internal audit finding but there would be little corrective action taken. ISO 9000 compliance raises documentation requirements for quality processes to a whole new level. An outside reviewer must certify that the enterprise is in compliance, and then the ISO reviewer can certify to the outside world that the enterprise is in compliance with the ISO standard. These compliance reviews are not one-time exercises; periodic update reviews are required.

To clarify, ISO 9000 is not just one standard but a series of "certifiable" standards and guidelines:

- **ISO 9001.** Certifiable standard dealing with design
- **ISO 9002.** Certifiable standard dealing with manufacturing
- **ISO 9003.** Certifiable standard dealing with manufacturing and assembly
- **ISO 9004.** Guideline defining a quality system

These standards are periodically updated with the current year appended to the standard; the just-released current version is known as ISO 9001: 2008. To add to the complexity, an enterprise can claim that it is only in compliance with an earlier version, ISO 9000: 1994. The QS 9000 series of standards are similar to ISO 9000 but pertain just to the automotive industry. A certifiable standard means it is subject to review by an outside auditor, as discussed. For purposes of this discussion, we will use the more generic term of ISO 9000 to refer to these quality management system standards.

ISO 9000 is a set of standards for a continual improvement-driven quality system, no matter whether a manufactured component or a service process. Exhibit 30.2 shows this quality management system process that is driven by internal procedures for continual improvements as well as customer requests. In this continual process, existing processes should be monitored, actions planned for improvements, and action items implemented for subsequent monitoring and further improvements. For many enterprises, the continual improvement quality process is nothing new. Internal auditors and systems development professionals have used essentially the same set of general processes since the early days of IT systems development, in what was called the Systems Development Life Cycle (SDLC),[2] a process to develop new IT information systems. However, those SDLC-developed applications called for a major amount of documentation that was often ignored by systems developers. Managers and IT developers often shrugged off the missing documentation with the claim that there were too many changes happening and they were just too busy. Many IT applications today are developed through more informal and iterative rapid application development processes than SDLC.

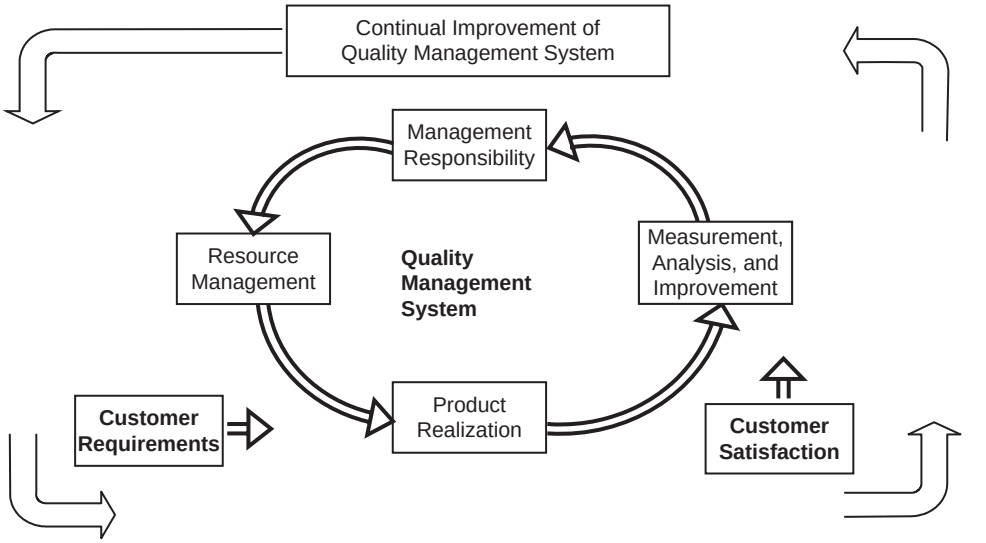


EXHIBIT 30.2 Quality Management System Process

Solid and accurate documentation is extremely important for an enterprise seeking to claim ISO registration. The issue here is that ISO registration has a global reach. When ISO 9001: 20000 section 4.2.3 states, among other provisions, that "a documented procedure should be established to define the controls needed" and "a) to approve documents for adequacy of issue," an enterprise or process documentation control system is needed to demonstrate compliance. ISO best practices call for a hierarchy of documentation in any area starting with top-level manuals to explain the What aspects down to instructions describing the Who and Where aspects of the practice. Exhibit 30.3 shows this documentation hierarchy with Documentation and Forms providing proof at the base. This documentation is essential to

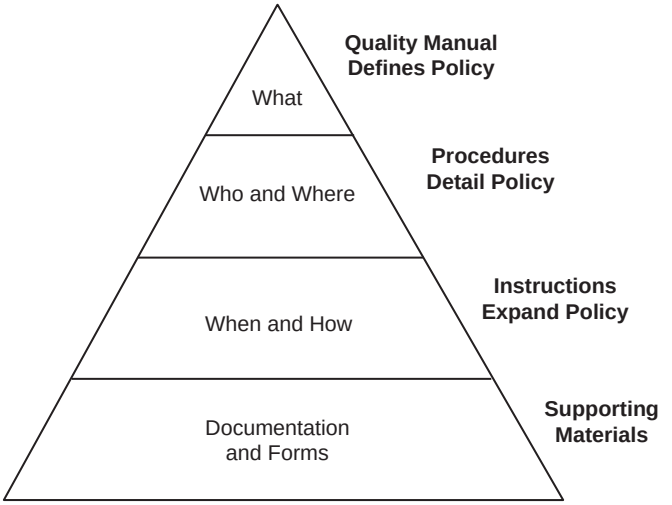


EXHIBIT 30.3 ISO Documentation Hierarchy

support a quality management system and certainly is required by external certification auditors.

These paragraphs have provided a very high-level description of the ISO 9000 quality management process. ISO 9000 is important for all types of enterprises to assert to their own internal management and to the outside world that they represent a quality-focused enterprise. To show the breadth of ISO 9000 certification, in 1995, the American Institute of Certified Public Accountants (AICPA) became the first major worldwide professional organization to become ISO 9001 certified.[3] Enterprises of all levels should consider adopting ISO 9000 processes.

The IIA, unfortunately, has not been aggressive in its communications regarding ISO 9000. At the time of this publication, only one article in the IIA's *Internal Auditor*[4] has suggested using ISO 9001 and 14001 in tandem with the Committee of Sponsoring Organization's (COSO's) internal control framework to help enterprises deal with risks that could impact their financial statements. In addition, in April 2008 the IIA used its Global Auditing Information Network (GAIN), as discussed in Chapter 11, to survey members on their involvement with ISO 9000 quality management processes. Thus, the IIA does not appear to have embraced ISO 9000 concepts as enthusiastically as, for example, the AICPA has. We expect this to change as internal auditors become more aware of the importance and impact of ISO 9000 quality management standards.

(ii) ISO 9000 AND SARBANES-OXLEY: COMMON THREADS Many financial managers and internal auditors may argue that they are busy enough with their Sarbanes-Oxley (SOx) compliance activities, and they may question why should they get involved with ISO standards. They might further argue that ISO quality management standards belong more on the production floor, and they are or should be more interested in SOx issues. William A. Stimson, a quality audit specialist, has compared SOx and ISO 9000 requirements and has found many common threads.[5] Chapter 2 of Stimson's book provides an overview of the SOx legislation and some of the common requirements by major sections of the SOx legislation and ISO 9000:

- SOx Title II on auditor independence is very similar to guidance in ISO 9001.
- SOx Title III on corporate responsibility for financial reporting (Section 302) is similar to the ISO 9001 requirements that the enterprise's executive committee must certify certain reports as true and also attest to their compliance with the report contents.
- SOx Title IV on financial disclosures (the often-dreaded Section 404) is similar to ISO 9001 on management's responsibility for the quality management system; both call for standards to certify that internal controls are effective and that there is a code of conduct in place.
- SOx Title VIII on corporate and criminal fraud accountability has similar requirements to the ISO 9001 rules on management's responsibility for records and documents.

Our aim here is merely to highlight areas where SOx and ISO 9000 rules have some similar requirements. Perhaps a major difference is that SOx comes with criminal penalties for noncompliance; the failure to achieve ISO standards primarily reduces an enterprise's competitive edge.

As with many ISO standards, ISO 9000 outlines requirements for the continuous improvements of an enterprise's quality management system. There is not just one

EXHIBIT 30.4 ISO 9001: 20000 Key Elements

- **0** Introduction
- **1.0** Scope
- **2.0** Normative References
- **3.0** Definitions
- **4.0** Quality Management System
  - **4.1** General Requirements
  - **4.2** Documentation Requirements
- **5.0** Structure and Responsibility
  - **5.1** Management Commitment
  - **5.2** Customer Focus
  - **5.3** Quality Policy
  - **5.4** Planning
  - **5.5** Responsibility, Authority and Communication
  - **5.6** Management Review
- **6.0** Resource Management
  - **6.1** Provision of Resources
  - **6.2** Human Resources
  - **6.3** Infrastructure
  - **6.4** Work Environment
- **7.0** Product Realization
  - **7.1** Planning of Product Realization
  - **7.2** Customer-Related Processes
  - **7.3** Design and Development
  - **7.4** Purchasing
  - **7.5** Production and Service Provision
  - **7.6** Control of Monitoring and Measuring Devices
- **8.0** Measurement, Analysis and Improvement
  - **8.1** General
  - **8.2** Monitoring and Measurement
  - **8.3** Control of Nonconforming Product
  - **8.4** Analysis of Data
  - **8.5** Improvement

set of attributes; the enterprise must accept inputs from customers in order to initiate continuous improvement processes. Exhibit 30.4 lists the high-level key elements of ISO 9000, with each of these sections supported by more detailed requirements. For example, section 4.0 on the quality management system requirements has a section 4.1 and 4.2 on general and documentation requirements followed by more detailed items, such as 4.2.3 on the control of records. However, Exhibit 30.5 on section 8.2.2,

EXHIBIT 30.5 ISO 9000 Standards Example: 8.2.2 on Internal Auditing

The organization *must conduct periodic internal audits* to determine if their Quality Management System conforms to ISO 9001, and has been effectively implemented and maintained. *Audit program planning* must take into consideration the status and importance of activities and *areas to be audited* and the *results of previous audits*. The audit procedure, scope, frequency and methodologies must be defined. These *audits must be performed* by personnel other than those who performed the activity being audited. Timely corrective action must be taken on deficiencies found during these audits, with follow-up actions including verification of corrective action implementation and reporting verification results.

Note: Italics added.

internal auditing, shows the nature and content of auditing requirements in these ISO standards. A lot of requirements are built into the single paragraph. *Auditing* here refers to the ASQ quality auditors discussed in Chapter 31, not necessarily the IIA-heritage internal auditors who have been the prime subject of most of these chapters.

(b) IT Security Standards: ISO 17799 and 27001

Two related IS management systems standards are discussed here, ISO 17799 and ISO 27001. ISO 17799 was first published in the United Kingdom as BS7799 in 1995; the standard has been updated over the years and is now known as IS0 17799: 2005, and it is scheduled to be renumbered as ISO 27002. For now, ISO 17799 represents an important IT-related security standard designed to help any enterprise that needs to establish a comprehensive IS management program or improve its current IS practices.

ISO 17799 is a standard about both *information* and IS in a general and all-inclusive sense. Since such information can exist in many forms, the standard takes a very broad approach and includes a wide range of security standards covering security regarding:

- Data and software electronic files
- All formats of paper documents including printed materials, handwritten notes, and even photographs
- Video and audio recordings
- Telephone conversations as well as e-mail, fax, video, and other forms of messages

The concept here is that all forms of information have value and need to be protected just like any other corporate asset. Many enterprises today do not even consider security standards in these broad areas, but the ISO standard suggests they should be covered when appropriate. In addition, the infrastructure that supports this information, including networks, systems, and functions, must also be protected from a wide range of threats, including everything from human error and equipment failure to theft, fraud, vandalism, sabotage, fire, flood, and even terrorism.

Like all other ISO standards, this published standard does not really prescribe *what* is specifically required but outlines areas where there are requirements for security-related standards. Exhibit 30.6 outlines some of the high-level standard areas taken directly from ISO 17799. The standard does not contain detailed requirements for each of these areas—to be a thorough and consistent international standard would require a huge, extensive text that certainly would not be all-inclusive and would soon be out of date. Rather, for instance, line 4.2 in the outline calls for security standards covering third-party access policies. ISO standards do not specify the details but call for an enterprise to have a documented and approved policy covering third-party access policies. Thus, the standard is somewhat of a heads-up type of checklist. An enterprise should develop its own sets of more detailed standards and procedures in this and other areas. Their type and extent can depend on many factors, but the ISO 17799–compliant enterprise should address this issue along with the other topic areas in the standard.

As a first step to implementing ISO 17799, an enterprise should identify its own IS needs and requirements. This requires performing an IS risk assessment along the

EXHIBIT 30.6 ISO 17799 Standards Topic Areas

1. Scope. A high-level description of the application of this standard.
2. Terms and definitions. Consistent with other ISO standards, all major terms are defined (e.g., definition of what is meant by "Confidentiality").
3. Standards or need for a high-level information security policy.
4. Requirements for an enterprise security organization
   - 4.1. Information security infrastructure
   - 4.2. Security and third-party access policies
   - 4.3. Outsourcing considerations
5. Asset classification and control standards
   - 5.1. Accountability for assets
   - 5.2. Information classifications
6. Personnel security
   - 6.1. Security considerations in job definitions and resources
   - 6.2. User training for personnel security
   - 6.3. Standards for responding to security incidents and malfunctions
7. Physical and environmental security including requirements for:
   - 7.1. Secure areas
   - 7.2. Equipment security
   - 7.3. General controls
8. Communications and operations management
   - 8.1. Operational procedures and responsibility
   - 8.2. System planning and acceptance
   - 8.3. Protections against malicious software
   - 8.4. Housekeeping
   - 8.5. Network management requirements
   - 8.6. Media handling and security
   - 8.7. Exchanges of information and software
9. Access control
   - 9.1. Business requirements for access control
   - 9.2. User access management
   - 9.3. User responsibilities for security standards
   - 9.4. Network access control
   - 9.5. Operating system access control
   - 9.6. Application access management
   - 9.7. Monitoring standards for systems access and use
   - 9.8. Mobile computing and related networking
10. System development and maintenance standards
    - 10.1. Security requirements hardware and software systems
    - 10.2. Application systems security
    - 10.3. Cryptographic controls
    - 10.4. Security of system files
    - 10.5. Security in development and support processes
11. Business continuity management standards
12. Security standards covering compliance issues
    - 12.1. Compliance with legal requirements
    - 12.2. Reviews of security policy and technical compliance
    - 12.3. Systems audit considerations

lines of the COSO enterprise risk management (COSO ERM) processes discussed in Chapter 6. Such an assessment should focus on the identification of major security threats and vulnerabilities as well as an assessment of how likely it is that each will cause a security incident. This process should help to pinpoint an enterprise's unique IS needs and requirements.

An enterprise should identify and understand all of the legal, statutory, regulatory, and contractual requirements that it and its trading partners, contractors, and service providers must meet. Doing so requires an understanding of an enterprise's unique legal information security needs and requirements.

ISO 17799 is the first of a series of international standards meant for any enterprise that uses internal or external computer systems, possesses confidential data, depends on IT to carry out its business activities, or simply wishes to adopt a higher level of security by complying with a standard. Although the standard is relatively new and not in common application, at least in the United States, compliance with it constitutes commitment to IT security in an enterprise, just as ISO 9000 compliance has become a guarantee of quality. Compliance should promote an increased level of mutual confidence between partners, where each can attest that it has established security standards in compliance with a recognized set of standards. In addition, as ISO 17799 compliance becomes more common for enterprises, it may result in potentially lower premiums for computer risk insurance; it certainly will yield better protection of confidential data and improved privacy practices and compliance with privacy laws. ISO 17799 is a structured and internationally recognized methodology that should help an enterprise to develop better management of IS on a continuing basis. It is a code of practice that supports the IS management systems requirements of the related security standard, ISO 27001.

(c) IT Security Technique Requirements: ISO 27001

While ISO 17799 is a high-level code of practice covering security controls, ISO 27001 is what ISO defines as the "specification" for an Information Security Management System. That is, this standard is designed to measure, monitor, and control security management from a top-down perspective. The standard essentially explains how to apply ISO 17799, and it defines the implementation of this standard as a six-part process:

1. **Defin a security policy.** A fundamental component of any standard is the need for a formal, senior management–approved policy statement. All other compliance aspects of the standard will be measured against this policy statement.
2. **Defin the scope of the ISMS.** ISO 17799 defines security in broad terms that may not be appropriate or needed for all enterprises. Having defined a high-level security policy, an enterprise needs to define the scope of its ISMS that will be implemented. For example, ISO 17799 defines element of security requirements as video and audio recordings. If this is not necessary for a given enterprise, it would be specifically excluded for its ISMS scope.
3. **Undertake a risk assessment.** The enterprise should identify a risk assessment methodology that is suited to its ISMS environment, then develop criteria for accepting risks and define what constitutes acceptable levels of risk.

4. **Manage the risk.** This is a major process that includes formal risk identification, risk analysis, and options for the treatment of those risks. The latter can include applying appropriate risk avoidance controls, accepting risks, taking other steps to avoid them, or transferring the risks to other parties, such as insurers or suppliers.
5. **Select control objectives and controls to be implemented.** This is the same audit and control process discussed elsewhere in this book, such as in Chapter 15 on planning and performing internal audits. For each defined control objective, the enterprise should define an appropriate controls procedure.
6. **Prepare a statement of applicability.** This is the formal documentation that is necessary to wrap up the ISMS documentation process. Such documentation matches control objectives with procedures to manage and implement the ISMS.

As can be seen from these steps, risk analysis and security policies are fundamental to this standard. While setting up these practices is not an internal audit matter, internal audit can provide strong help to IT management by offering to serve as an internal consultant and helping to perform adequate risk assessment procedures. The roles of internal audit acting as an enterprise consultant are discussed in Chapter 28.

Because of strict ISO copyright rules, we have not supplied lengthy excerpts of ISO 27001. However, the example in Exhibit 30.5 shows the standard as tight and unambiguous text. There is little specific detail but enough to allow an enterprise to implement its ISMS. The formal standard concludes with an appendix section listing control procedures for each of its objective details. ISO 27001 should not be considered to be a comprehensive set of control procedures they will change as technology changes; rather, it is an outline for the framework of an ISMS that should be continually implemented, monitored, and maintained.

(i) **THE FUTURE** ISO 17799 (soon to be renamed ISO 27002) and ISO 27001 are already global standards, with established compliance and certification schemes in place, particularly in the United Kingdom and European Union. Both of these standards will continue to evolve, to track technology, and will expand. We can expect them to be more closely tied with control frameworks such as CobiT (*C*ontrol *ob*jectives for *i*nformation related *T*echnology, a framework for managing IT and general internal controls discussed in Chapter 5) in the future. There can be little doubt that these ISO IT security standards will continue to grow in their influence and adoption will continue to expand.

Internal auditors should monitor the status of ongoing progress of these IT security standards; doing so calls for appropriate ISMS within the IT function. While an IT function can delay fully implementing ISO 27001, 27002, and an ISMS, some vendor or other major stakeholder may demand evidence of the enterprise's compliance with this standard. Internal audit can often be of help with such matters.

(d) Service Quality Management: ISO 20000

Many professionals will agree that we live in a world with too many standards, many of which are similar to others but are not connected to each other. ISO 20000 on service quality management introduces some much-needed standards convergence. This is an international standard for IT service management, and it introduces many

of the ITIL service management best practices that were discussed in Chapter 18. The standard consists of two parts, Part I on implementing service management and Part II describing best practices for service management. The Part I standard specifies the need for a series of service management documented processes, such as defining requirements for implementing such a management system; new or changed service requirements; and documented relationship, control, resolution, and release processes. Quite correctly, the standard takes the best practices approach of ITIL and calls for formal documented processes to support them as part of ISO 20000.

ISO 20000 calls for an enterprise to adopt and certify that it has adopted the ITIL best practices discussed in Chapter 8. Formally, this standard "promotes the adoption of an integrated process approach to effectively deliver managed services to meet the business and customer requirements." ISO 20000 is the first global standard for IT service management and is fully compatible and supportive of the ITIL framework. It will undoubtedly have a significant impact on the use and acceptance of ITIL best practices and the whole IT service management landscape.

In future years, internal auditors should see an increasing level of recognition of the importance of ISO service-related standards. In our increasingly global economy, no matter what national world trade restrictions may be imposed, internal standards are needed to define common practices and to better facilitate communication. When an enterprise or service organization anywhere in the world has achieved ISO 9000 quality management certification, customers and users can expect a certain minimum level of documentation and process standards. The ISO 27001 IT security standards should soon reach a similar level of importance and recognition. We should see increasing convergence trends between ISO and standards in other areas. Internal auditors at all levels should understand and embrace these important ISO standards.

30.3 ISO 19011 Quality Management Systems Auditing

Every ISO standard discussed here contains references to the need to audit a particular quality system, such as ISO 9000 on quality management or ISO 14000 on environmental management systems. Each of these published standards offers resources for an enterprise to "save time, effort and money" in its management systems auditing processes. The ISO 19011 quality management systems auditing standard very much relates to the ASQ quality audit standards discussed in Chapter 31, and it outlines four critical decision/support resources for the efficient planning, conduct, and evaluation of quality and/or environmental audits:

1. The need for a clear explanation of the principles of management systems auditing
2. Guidance on the management of audit programs
3. Guidance on the conduct of internal or external audits
4. Advice on the competence and evaluation of auditors

Since these topics are discussed in other chapters, you may wonder why an ISO international standard is needed here. This standard is directed at quality auditors worldwide, including many who have not been exposed to modern internal

auditing (discussed in Chapters 1 and 2) and the IIA's *International Standards for the Professional Practice of Internal Auditing* (outlined in Chapter 8).

This ISO standard outlines five principles of auditing:

1. **Ethical conduct.** Auditors performing ISO 19011 audits should be honest and do the right thing.
2. **Fair presentation.** Auditors should be evenhanded when reporting results.
3. **Exercise due professional care.** Auditors should do what is reasonable and normally expected.
4. **Independence.** Auditors should avoid conflicts of interest to ensure their integrity.
5. **Evidence-based approaches.** Auditors should investigate first and then report the facts.

The ISO 19011 standard contains a detailed set of the principles of auditing from an ISO, quality audit perspective. Exhibit 30.7 shows the ISO 19011 auditing principles and related subheadings. There are some duplicate titles in these subheadings, as the standard places some topics, such as the audit report, under multiple audit principles. This is a very comprehensive overview of internal auditing from a quality

EXHIBIT 30.7 ISO 19011 Auditing Principles and Subheadings

- **Ethical Conduct**
  - Audit Team
  - Audit Plan
  - Work Documents
  - Opening Meeting
  - Audit Report
  - Report Distribution
  - Personal Attributes
- **Fair Presentation**
  - Findings
  - Audit Report
  - Personal Attributes
  - Outcomes
- **Due Professional Care**
  - Audit Report
  - Auditor Judgment
  - Findings
  - Conclusions
- **Independence**
  - Selecting Auditors
  - Assigning Work
  - Follow-Up Activities
- **Evidence-Based Approach**
  - Collecting Evidence
  - Findings
  - Conclusion
  - Audit Report

audit perspective. While space in this chapter does not allow a detailed summary of this ISO standard, virtually all of the ISO 19011 related to internal auditing principles are described in other chapters.

As mentioned earlier, the IIA sent out a survey in April 2008 over its GAIN network to assess internal auditor involvement with ISO 19011. Of the 1,500 surveys that were sent out, only about 150 were returned. The results generally showed that IIA internal auditors have little involvement with the quality auditors—described in Chapter 31—who would be responsible for implementing this ISO standard. Based on the survey results,[6] 70% of the IIA members stated that there was no involvement with ISO 19011 in their enterprises.

30.4 ISO Standards and Internal Auditors

As enterprises become more and more global with many commerce interconnections and relationships, ISO standards become more important. While standards describing component dimensions—such as the tread pattern and size on a bolt—are essential for commerce, the "softer" quality system standards, such as ISO 9000, are equally important. Enterprises in one location will refuse to do business with enterprises elsewhere unless they can certify their compliance to some ISO standard. Chapter 33 also discusses the potential future internal audit significance of the ISO 100011 quality auditing standard.

Although many IIA-heritage internal auditors have not followed ISO standards and quality auditing in the past, we expect this to change. For example, the GAIN survey shows that the IIA is at least thinking about incorporating the new ISO 19011 quality auditing international standard in its guidance materials.

Internal auditors should develop a CBOK level of general understanding of such ISO standards, such as 9000 for quality and 19001 for auditing. In addition, where specific standards are used in an internal auditor's enterprise, such as for product manufacturing, an internal auditor should learn more about them and how they are being implemented and audited. In the future, an understanding of appropriate ISO standards should be a key internal auditor knowledge requirement.

Notes

1. The abbreviation is ISO because of its French spelling.
2. There are numerous published references to the SDLC process. A Google search on SDLC system development will get the reader started.
3. www.qualitydigest.com/june99/html/body_iso_9000.html.
4. Sandford Liebsman, "Quality in the Mix," *Internal Auditor* (October 2005).
5. William A. Stimson, *ISO 9001 & Sarbanes-Oxley: A System of Governance* (Chico, CA: Paton Press, 2006).
6. Institute of Internal Auditors GAIN Network, "International Organization for Standardization (ISO) 9001: 20000 Quality Management System Type: Executive Summary Report," April 10, 2008.

CHAPTER 31

Quality Assurance Auditing and ASQ Standards

The main focus of this book has been on internal audit standards and activities of the Institute of Internal Auditors (IIA), of Certified Internal Auditors (CIAs), and of certified public accountant (CPA)–type external auditors. However, these are not the only professionals who consider themselves auditors. There are many other audit professionals, including U.S. federal government contract auditors and professionals who audit healthcare and hospital standards. These other auditors typically do not work in or with the corporate headquarters offices that are the domains of IIA-associated internal auditors or even the CPA-type external auditors. Although the IIA-member or heritage internal audit professional, discussed throughout this book, often does not have a strong working relationship with them, quality auditors play an important role in many enterprises. Administered through the American Society for Quality (ASQ) professional organization, they are a unique internal audit–like professional group that has its own standards, codes of ethics, and professional certification designations. Once called quality auditors rather than just internal auditors, these professionals have responsibilities to review a wide range of ISO standards in the enterprise in regard to compliance, work simplification, and quality-related processes. Quality auditors have historically primarily operated on the shop floor in manufacturing enterprises.

Today quality auditors are becoming closer to IIA internal auditors. More accurately, each of these internal audit professional groups is changing in terms of objectives and approaches in ways that bring them closer together. The classic IIA internal audit professional should have an understanding of the activities of quality auditors and how their work fits in the overall environment of corporate governance.

This chapter reviews the role of quality auditors in an enterprise, their practices and standards. There are many similarities between the activities of these auditors and IIA internal auditors. With a growing convergence of enterprise activities to improve governance and internal controls, we can expect to see these two internal audit groups become more closely aligned. IIA-type of internal auditors should have a general common body of knowledge (CBOK) need for understanding the roles, responsibilities, and activities of quality auditors.

In addition, we also introduce quality-assurance (QA) reviews of an internal audit function performed by members of the internal audit team themselves or by contracted outside reviewers. A quality auditor is a separate professional who is a member of the ASQ. Quality assurance, or QA, refers to a process practiced by many

internal audit functions. Larger internal audit functions, in particular, often bring real value to their overall enterprise by having an independent quality review of their internal audit practices and operations.

31.1 Duties and Responsibilities of Quality Auditors

For many traditional, IIA-heritage internal auditors, terminology can be a bit confusing. While some quality auditors may belong to the IIA as well, they have their own separate professional organization, the Quality Audit Division (QAD) of the ASQ. The ASQ professional organization, with responsibilities for many activities in quality management, previously referred to its QAD professional affiliates as "quality auditors." The ASQ now refers to audit members as just internal auditors. Confusing? Yes. In this chapter, we refer to the ASQ professionals as quality auditors to distinguish them from internal auditors.

The ASQ is the leading proponent of the quality movement in the United States. It has a wide range of publications, professional certifications, and separate divisions covering industries such as aerospace and pharmaceuticals as well as professional practices. The ASQ is very involved with the ISO quality standards in the United States, discussed in Chapter 30, and its QAD is responsible for compliance audits against those ISO standards.

The QAD's stated mission is "To support auditors and other stakeholders by defining and promoting auditing as a management tool to achieve continuous improvement, effective communication, and increased customer satisfaction." Again, the use of just "auditor" causes some confusion regarding the roles of these quality auditors. In addition, the ASQ and its QAD recognizes and defines several activity levels of auditing:

- **Self-audits.** This is a quality audit performed within the enterprise to review compliance with ISO quality standards and the like.
- **Second-party audits.** Quality auditors often perform reviews to assess whether their suppliers are operating in compliance with some specified standards. A second-party audit occurs when an enterprise's own quality auditors visit a supplier to test compliance with some standards.
- **Third-party audits.** This is an audit performed at the enterprise by an independent organization, such as one of the ISO registrars, discussed in Chapter 30, or an auditor from a government agency, such as the Department of Labor's Occupational Safety and Health Administration (OSHA) or the Federal Drug Administration (FDA).

As discussed, although the ASQ historically used the term *quality auditors,* it uses *auditors* today. This change is due to the ASQ broadening its own professional designations. Exhibit 31.1 describes the classifications of quality audits showing both outside customers, who need quality audit assurances, and suppliers. These areas of activity put quality auditors in a different framework from IIA internal auditors.

Quality audit terminology becomes even more confusing because the ASQ designates its audit professionals as internal or external auditors. An ASQ internal auditor reviews controls and standards within that auditor's enterprise or employer. An ASQ external auditor, in this context, performs third-party reviews at other enterprises

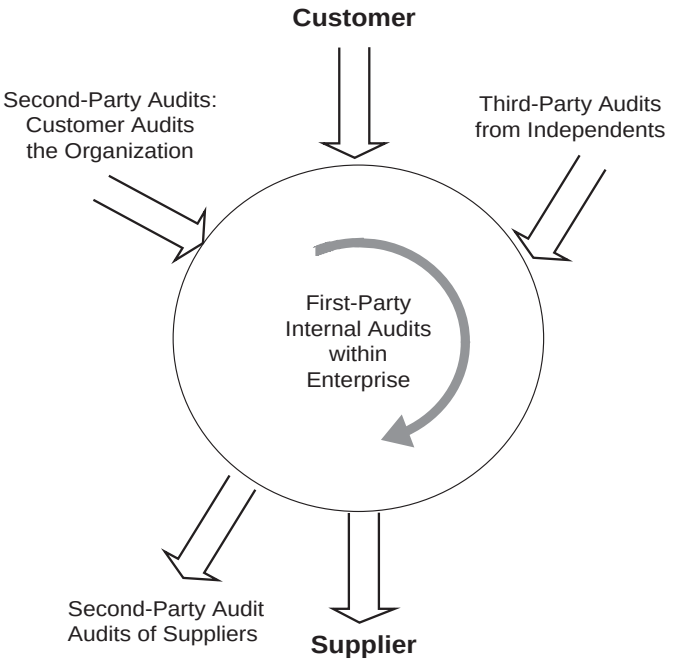


EXHIBIT 31.1 Classifications of Quality Audits

to establish such matters as ISO certifications. While a quality auditor may be a member of the IIA in addition to the ASQ, the designation of an *external* quality auditor has no regular relationship with the financial statement attest auditors, the designation of the American Institute of Certified Public Accountants (AICPA). We generally use the term *quality auditor* for all references to these ASQ-background auditors to make a distinction between IIA-heritage internal auditors.

The IIA has its Certified Internal Auditor (CIA) professional designation, the Information Systems Audit and Control Association (ISACA) has its Certified Information Systems Auditor (CISA) designation, and the ASQ also has the Certified Quality Auditor (CQA) professional certification. Chapter 27 outlined these internal audit professional certifications. In addition to holding a CQA, a quality auditor may earn several quality audit specialty subdesignations, such as for hazardous analysis or biomedical auditing. These certifications require designated levels of work experience and successfully passing an examination. ASQ quality auditors are involved in similar professional activities and have standards similar to IIA internal auditors. In addition, the ASQ has a series of specialized national meetings and conferences for ASQ quality auditors.

31.2 Role of the Quality Auditor

ASQ procedures, standards, and quality auditing guidance materials are similar to the standards used by IIA internal auditors. Quality auditors follow many of the same general internal audit steps as IIA-sponsored internal auditors in their procedures for developing programs, reporting findings, and the like. Quality auditors usually

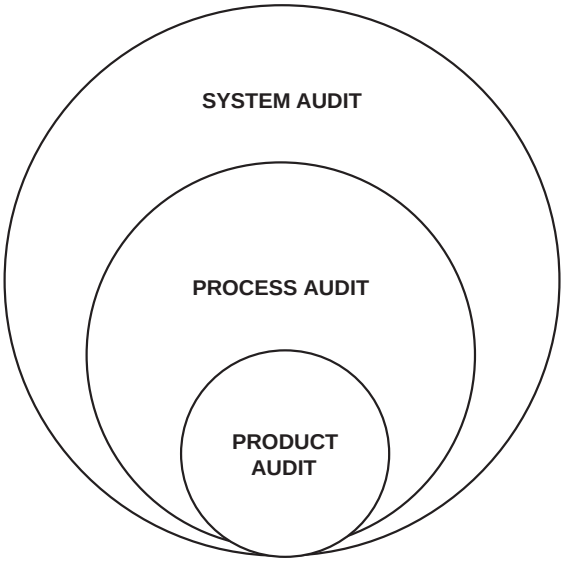


EXHIBIT 31.2 Types of Quality Audits

are not involved with audit issues such as reviews of financial internal controls nor are they directly involved with audits covering many information technology (IT) internal controls area. Quality auditors often follow published international industry standards, such as ISO 9000, and their audits often tend to be much more quantitative and mathematical than the work of the typical IIA-heritage internal auditor. The work of quality auditors is often closely aligned with the classic processes used by manufacturing production quality assurance specialists.

Quality audits include terminology that may be unfamiliar to IIA-heritage internal auditors and the managers accustomed to working with them. For example, Exhibit 31.2 shows that quality audits can be designated as product, process, and system audits based on their scope and objectives.

- A *product audit* is an assessment of a final product or service and a review of its "fitness for use" against stated requirements or specifications. In a manufacturing sense, a product audit would be performed on some item that has just passed its final inspection and is ready for delivery to the customer.
- A *process audit* is the major type of audit performed by quality auditors. This is a review to verify conformance to standards, methods, procedures, or other requirements.
- A *systems audit* is *not* an IT-related systems review but an audit that covers all aspects of a control system. This type of review is conducted to verify, through objective evidence, that all aspects of management systems and organizational plans are implemented to adequately meet identified requirements.

Quality audits are typically more analytical in their approaches than the usual IIA type of internal audit. Because many quality auditors are more engineering technicians than accountants, they tend to make greater use of analytical tools and techniques in their workpaper analyses and audit reports. Perhaps because many quality audits are performed in process and manufacturing environments, many

quality auditors are often much more production-shop-floor–oriented than many IIA-heritage internal auditors. An explanation is that today a quality audit function often does not report to the CAE and the audit committee but typically has strong ties to production operations.

Quality audit tools and techniques are also often different from those used in IIA-heritage internal audits. An example might help explain the differences: Exhibit 31.3 shows a Pareto chart, a common diagram used in quality-related audit analyses. A Pareto chart ranks the types of errors or problems found by the auditor on the vertical axis with the most severe problems listed first. In this example, there were 62 cases of defect 1 during the period reviewed. Similarly, there were 58 cases of defect 2 with increasingly fewer cases for the other defects. The numbers of cumulative defects are plotted on the vertical axis. The line goes from 62 to (62 + 58 = 120) for the second point and continues. The idea behind a Pareto chart is to see which defects require the most attention. The less than 10 instances of defect 6 shown here should require less management attention.

While quality auditors have traditionally used tools such as Pareto charts to review quality defects and make recommendations, the recent worldwide movement to ISO 9000 quality standards has very much changed the role of quality auditors. Internal audit requirements are common in most of the ISO standards discussed in Chapter 30. For example, subsection 8.2.2 of ISO 9001: 2000, describes the requirements for internal audits of ISO standards. It also calls for management to conduct internal audits at planned intervals to determine whether the quality management system conforms to requirements of the standard and is implemented and maintained effectively. These standards also contain requirements for audit programs, management's responsibility, and other matters. Similar audit requirements exist for

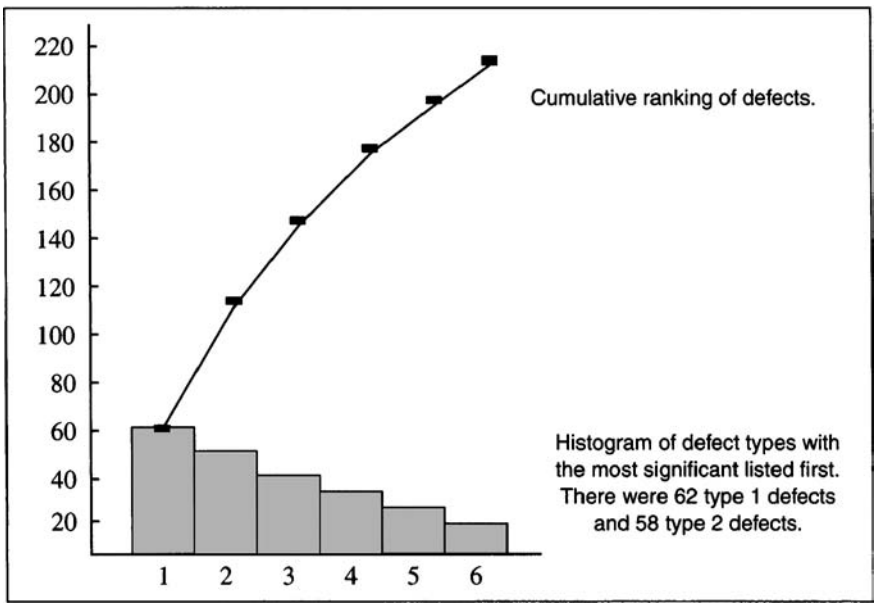


EXHIBIT 31.3 Pareto Chart Example

Source: Used with permission. Robert Moeller, *Brink's Modern Internal Auditing*, 6th ed. (Hoboken, NJ: John Wiley & Sons, 2005), p. 651.

EXHIBIT 31.4 ISO 9000 Standards Example: 8.2.2 on Internal Auditing

The organization must conduct periodic internal audits to determine if the QMS conforms to ISO 9001 and has been effectively implemented and maintained. Audit program planning must take into consideration the status and importance of activities and areas to be audited and the results of previous audits. The audit procedure, scope, frequency, and methodologies must be defined. These audits must be performed by personnel other than those who performed the activity being audited. Timely corrective action must be taken on deficiencies found during these audits, with follow-up actions including verification of corrective action implementation and reporting verification results.

Source: ISO 9001: 2000 Subsection 8.2.2 www.ISO.org.

other quality management system ISO standards. Those quality audit principles are also described in ISO 19011, also highlighted in Chapter 30. Referring to Chapter 20 on ISO standards, Section 6 of ISO 27001: 2000, for example, is titled *Internal ISMS Audits*. The ISO standard states, among other things:

> *The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS:*
>
> ***a.*** *conform to the requirements of this International Standard and relevant legislation or regulations;*
> ***b.*** *conform to the identified information security requirements;*
> ***c.*** *are effectively implemented and maintained; and*
> ***d.*** *perform as expected.*

Again, this section of the standard has more substance than shown here, but the extracts are presented to illustrate the requirements of audits for ISO standards. Any enterprise that is launching and seeking standards certification must establish a quality audit function.

Quality audit functions are often organized more informally than those of IIA-trained internal audit functions with their audit committee reporting relationships to the board of directors. The next sections discuss this quality audit process. Currently there is almost a disconnect between quality auditors following ASQ standards, and the IIA internal auditors following internal audit professional standards. Over time, however, we should see a greater level of convergence between these auditing processes.

Quality auditors are often involved with tests for improvement based on their findings from earlier reviews. To accomplish this continuous improvement, the data in a new review must be analyzed for trends and weaknesses. The quality auditor then compares results to goals and objectives, and analyzes process data to identify risks, inefficiencies, opportunities for improvement as well as negative trends. The results may be recommendations for changes in procedures or in other elements of the process, such as improvements in acceptance criteria or methods of monitoring. Suggested changes in equipment or technology may also be among the quality auditor's scope of identifying areas for continual improvement. In many respects, quality auditors often recommend more significant changes to the improvement cycle than has been the case of internal auditors.

31.3 Performing ASQ Quality Audits

Many professionals clearly recognize traditional internal auditing standards. The IIA's *International Standards for the Professional Practice of Internal Auditing,* discussed in Chapter 8, provide a good overview of those standards and discusses the overall profession of internal auditing. The ASQ-sponsored practice of quality auditing brings a somewhat different perspective to auditing. Although it has its roots in earlier quality assurance and industrial engineering processes, quality auditing is particularly important for measuring compliance to ISO standards, and there are both internal and external components into this auditing practice.

ASQ-driven audits—quality audits—are somewhat different from many IIA internal controls–oriented audits They are reviews performed to assess regulatory compliance rules or to meet requirements for ISO standards registration or certification. They are also important because they are a key feedback loop in an enterprise's quality system to keep management informed about compliance with documented systems procedures. As discussed, quality audits are further characterized as what are called internal or self-audits and then second- or third-party audits. Under these rules, a quality audit may be performed, as a self-audit, by persons very close to the actual process operations. Quality audits are typically not performed by a separate internal audit department but by persons in the enterprise who can demonstrate a level of objectivity.

In addition to the internal or self-audit, second- or third-party audits may occur. Quality audits take place in the ISO standards environment where an enterprise must check that its suppliers and others are in compliance with the standards under review. Second-party audits occur when an enterprise performs a quality audit on one of its suppliers. A third-party audit occurs when an outside registrar performs an independent review. The concept here is that an enterprise must determine that its suppliers are in compliance with some standard through a second-party review. However, in order to hold itself out to others that it is in compliance with a standard, such as ISO 90001, the enterprise must contract with a certified independent registrar to certify that compliance.

Many quality auditing processes are based on the principles first established by W. Edwards Deming in Japan in the years following World War II. We already have discussed how the originator of this volume, Victor Brink, launched internal auditing in the years following the war. Deming worked as a consultant in postwar Japan to help repair and rebuild the country's shattered manufacturing resources. Deming introduced many quality management techniques that were initially ignored by U.S. manufacturers, but those same techniques led to very high quality and innovative Japanese products, such the offerings of Toyota or Sony.

Although it is very simple in thought, a basic concept in Deming's work and a component of quality auditing activities is his plan/do/check/act (PDCA) cycle. Illustrated in Exhibit 31.5, this is a continuous improvement cycle where a team of quality auditors, among others, would work to improve processes. The team would use the PDCA cycle to review a process by following five steps:

Step 1. Plan. What are the objectives of a quality audit team? What changes are desirable, and what data are needed? What types of tests are needed? How will operations be observed?

Step 2. Do. Carry on or execute the planned tests.

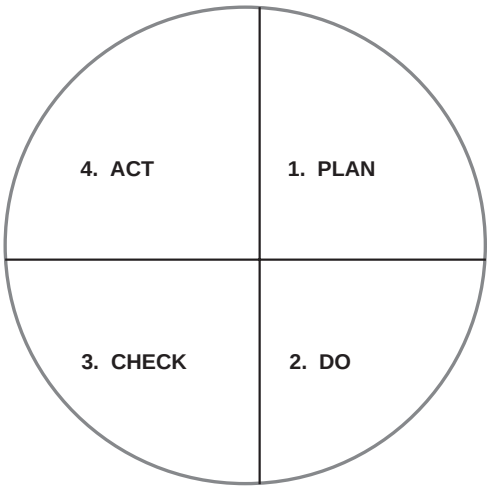


EXHIBIT 31.5 PSCA Cycle

Step 3. Check. Observe the results of tests to develop preliminary conclusions.
Step 4. Act. Study all test results to assess what was learned and what can be predicted from the exercise. Based on these results, determine areas for process improvements.
Step 5. Repeat steps while gaining more knowledge.

This simple method for process improvement is quite different from the traditional internal audit steps discussed in Chapter 7. A quality audit emphasizes process improvement. Quality auditors do not just review an area and then report results through a formal audit report. Rather, they look at some area, evaluate their findings, and then return and help to improve the process.

ASQ quality audits are often much more extensive than traditional IIA-heritage internal audits. Quality auditors are often interested in compliance with applicable standards with objectives to:

- Verify that the implemented system is working
- Verify that supporting training programs are cost effective
- Identify people or groups not following procedures
- Provide evidence to management and others that processes are working as documented

The quality audit process follows steps that are similar to IIA-heritage internal audits, but they are not supported by the same level of detailed internal audit standards found with IIA-heritage standards. The quality auditing process is often much more analytical than IIA-heritage internal audits. The Pareto chart in Exhibit 31.3 is an example of a typical procedure that quality auditors might use to develop their audit findings. A typical quality audit often emphasizes statistical analysis and analytical techniques much more than IIA-heritage internal audits.

Quality audits are launched and performed much like IIA-heritage internal audits. Quality auditors develop an audit plan, then perform the audit procedures

EXHIBIT 31.6 Quality Audit Process Steps

- Preaudit Activities
  1. Preparation for audit: Establish audit objectives.
  2. Planning for all audit activities.
- On-Site Audit
  1. Opening meeting: Meet with auditee and outline planned procedures.
  2. Audit: Activation will depend on the nature of the review.
  3. Closing meeting: Discuss findings and present draft report at end of fieldwork review.
- Postaudit Activities
  1. Audit report: Report on findings and recommendations.
  2. Management review: Discuss audit results with all levels of management.
  3. Corrective actions: Negotiate plan to correct audit findings.
  4. Follow-up/corrective action audits.

outlined in the plan, and finally conclude with an audit report emphasizing steps to achieve corrective actions. Exhibit 31.6 outlines these quality audit process steps, which are very similar to those used in IIA internal audits or some financial audit. A major difference is that quality auditors are much more involved with correcting audit findings and launching corrective action initiatives. In contrast to the IIA professional standards discussed in Chapter 8, quality auditors often assess control weaknesses and consult to help with implementing corrective actions.

As compliance with a growing number of ISO standards becomes more important, we will almost certainly see the role of the quality auditor moving more to an enterprise's front office. Audit committees and management will increasingly realize that there are many common needs for both ASQ-trained quality auditors and IIA-trained internal auditors. We will almost certainly see these two professional groups move closer together in future years.

31.4 Quality Auditors and the IIA Internal Auditor

There is an evolving level of integration today with IIA internal auditing and ASQ quality auditing. The term *quality auditing* is being replaced by just *auditing* in ASQ publications and in some ISO standards. The terminology used in both IIA and ISO standards is becoming increasingly consistent with revisions to each over recent years. ISO has defined an audit as a "systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled."[1] The IIA's definition of internal auditing, discussed in Chapter 7, contains some quality-related words: assurance, adding value, risk management, systematic, disciplined, control, and process orientation. Some integration appears to be taking place in terminology toward a generic assessment and business process improvement model.

There will probably be a growing convergence of internal auditing and quality auditing over the upcoming next years. An increasing number of enterprises worldwide are seeking ISO registrations, and ISO 9000 standards are becoming more process oriented, customer focused and business driven. With an emphasis on

"effectiveness," an ISO 9000–registered company must demonstrate its quality system effectiveness.

In some enterprises today, the chief audit executive (CAE) also is involved with an enterprise's quality audit function on at least a courtesy level. In the future, internal audit functions will almost certainly become more aware of the activities of their quality audit functions and should consider sharing resources. Although their historical roots are different, both audit functions should become involved with value-added audit functions for the enterprise. IIA-heritage internal auditors should develop a greater understanding of quality audit procedures, and the two audit groups should build regular and ongoing communication links. While each has a different approach and objectives, there may some value to sharing ideas and even doing some joint review work.

31.5 Quality Assurance Reviews of the Internal Audit Function

Internal auditors have a special role in their service to the management of the modern enterprise. As has been described in many chapters of this book, internal auditors visit a unit or component of an enterprise, review its controls, and make recommendations for improvements. The IIA-oriented modern internal auditor uses the *International Standards for the Professional Practice of Internal Auditing*, described in Chapter 8, as well as the supporting practices and procedures discussed elsewhere. Other members of the enterprise and potential auditees should understand that internal audit will be following good practices when it performs its reviews. However, beyond a high-level review of internal audit activities by their external auditors, no one regularly audits the internal auditors to see if they are following both good practices and their own professional standards.

The effective modern internal audit function should look at itself from time to time to determine if all of its own components are following good internal audit practices and procedures. This is best accomplished if internal audit goes through an audit-the-auditors type of review over its own functions. The *International Standards for the Professional Practice of Internal Auditing* refer to *quality-assurance reviews*. IIA standard 560 calls for the CAE "to establish and maintain a quality assurance program" to appraise the quality of the audit work performed through ongoing supervisory reviews, reviews by internal audit of its own work, and reviews by external parties. Chapter 11 discussed the concept of internal auditor control self-assessments where internal audit reviews its activities on a more informal basis.

In addition, and perhaps even more important, IIA standard 1312 "requires every internal audit department to have an external quality assessment at least once every five years by a qualified independent reviewer from outside the organization." In other words, in addition to its own internal quality assurance review function, internal audit must arrange for another independent internal audit entity or contract with an outside provider to assess the overall quality of the internal audit function. This is a key requirement for all internal audit departments.

Internal audit QA reviews are a special type of audit—more than a normal management assessment of operations or an external auditor Statement on Auditing Standards No. 70[2] external service organizations review. While the IIA standard 560 calls for three levels of review, this chapter primarily focuses on reviews of internal audit performed by normal internal audit operations, including members of other

enterprises or even a specialized department within internal audit. These reviews allow an internal audit function to assess the quality of its own procedures and its compliance with internal audit standards. This section describes the elements that should be included in an internal audit QA program and describes how internal audit can establish a program to perform these reviews.

(a) Benefits of an Internal Audit Quality-Assurance Review

Internal audit departments sometimes are viewed as operating outside of other mainstream enterprise functions. Internal audit reports to the audit committee with close ties with very senior levels of management and has contact with all other functions in the enterprise through its operational and financial reviews. However, as a very specialized function, internal audit is not always considered when other enterprise-wide performance measurement policies and procedures are established. This is not to suggest that internal audit is ignored. However, a new enterprise program of employee incentive pay, a major QA initiative, or some other employee benefit does not always consider the unique aspects of the internal audit function when designing these example inititives. These programs often are focused on the enterprise's main functions, whether they are manufacturing, distribution, or financial.

As a key supporting function in the enterprise, however, internal audit needs a way to measure itself and to establish incentives to do a better job. This is one of the real benefits of an internal audit QA review. While internal audit itself is the prime beneficiary of these reviews, other stakeholders in an enterprise also benefit from a strong program of internal audit QA reviews. These reviews allow internal audit to demonstrate to management that it is doing a good job or taking corrective action to improve if necessary. Other parties, such as regulatory agencies, also may benefit from these reviews, which provide a basis to better utilize the work of the internal audit department.

(i) BENEFITS TO INTERNAL AUDIT The main beneficiary of any internal audit QA review program will be internal audit itself. As highlighted in Chapter 1, internal audit operates somewhat differently from many other functions in a typical enterprise and cannot evaluate itself by such common measures of success as sales, production, or administrative efficiencies. An external reviewer who understands the internal audit process and who has had exposure to other enterprises can review internal audit operations from the perspective of internal audit's compliance with professional standards and by how its operations compare with those of other similar internal audit enterprises. A review of compliance with internal audit standards also is valuable. While an internal audit function should have a program in place to follow these standards in all of its auditing activities, compliance with one or another specific standard may slip through inattention or just the pressure of completing audit projects. A QA review will allow a reviewer outside the day-to-day internal audit activities to assess how good a given internal audit function is doing in complying with internal audit standards. This can be a valuable benefit to the modern internal audit function.

Internal audit also can benefit from being compared with other internal audit functions. Internal audit management does not always know how well it compares to other internal audit groups in terms of such things as its use of audit automation,

efficiency in performing audit tests, or travel policies. CAEs can gather some of this information through their professional contacts at IIA meetings or other personal or professional contacts. However, these contacts do not always provide the same level of objectivity that would be found through the work of an independent reviewer who looked at several internal audit enterprises. Even though one-to-one professional contacts are valuable, professional peers can gloss over faults or weaknesses when comparing activities.

Internal audit QA reviews, performed by outside parties, can point to areas where some audits were performed in a manner not fully in compliance with standards or where better efficiencies could have been achieved. For example, the sample selection approach used in a given audit may have been too large. Although the audit's results were correct, a smaller sample might have produced the same audit conclusions but with greater efficiency. As a result of such QA reviews, internal audit management may be able to improve its own overall operations.

(ii) BENEFITS TO MANAGEMENT Several levels of management, ranging from the managers directly responsible for internal audit areas reviewed to the audit committee, benefit from internal audit QA reviews. Although an internal audit team should not show its latest QA review report to the auditee management of the next audit project, the findings of a good program of QA reviews should result in better and more efficient audits. All members of management—and managers directly responsible for units audited, in particular—will benefit from an efficient and effective internal audit function. A program of QA reviews should help to ensure ongoing audit efficiency and effectiveness.

The audit committee and senior management should realize even greater benefits from a strong program of internal audit QA reviews. As has been discussed throughout this book, internal audit is a strong component in the system of internal controls. Senior management and the audit committee should understand the overall principles of internal control but may not always fully understand the workings of their internal audit function. Internal audit shares the summary results of its QA review with various levels of senior management. This information provides senior management with a greater confidence in the quality of the internal audit reviews performed. This is a major benefit to the overall enterprise.

(b) Elements of an Internal Audit Quality-Assurance Review

An internal audit QA review is a formal process similar to many of the audit procedures outlined in other chapters. The review should be properly planned, follow a formal audit program, and be performed by qualified reviewers who have an appropriate level of independence. Whether performed by a special unit of internal audit charged with performing such reviews or by an outside consultant, the review should follow the same standards of independence and objectivity found in any internal audit. The only significant difference here is that the QA review will focus its efforts on its own internal audit procedures. Similar to beginning any internal audit, establishing requirements for the review is an important first step necessary to launch an internal audit quality-review function. Although management may want to vary the content of any review to reflect local concerns within an enterprise and its internal audit function, the review should concentrate on the internal audit's

compliance with IIA standards. Any QA review should assess compliance with the principles outlined in those standards.

The specific details behind how the quality of internal audit operations will be measured depends on many factors, including the size of the internal audit department, directions by the audit committee and senior management specifying more emphasis on one area over another, and other factors. Nevertheless, all internal audit activities should be measured against compliance with these IIA standards.

A QA review usually begins with a detailed review of compliance with internal audit procedures. This would include evaluating the risk-assessment planning process; reviewing other planning documents and staff assignment procedures; and reviewing selected workpapers and reports used in actual audits, and all other planning and administrative materials used by internal audit in the course of performing its audit assignments. The purpose of this review approach is to measure the overall quality of internal audit's own procedures. While the specific procedures to be performed will vary with the size and activities of the internal audit department, Exhibit 31.7 outlines the general procedures of an internal audit QA review. In addition to reviewing workpapers and administrative procedures, the QA review should focus on auditees who either requested reviews or have had reviews performed in their areas. An internal audit function contributes little to the quality of procedures in the overall enterprise if auditee management has serious

EXHIBIT 31.7 Procedures for a Quality-Assurance Review of Internal Audit

1. Define the areas to be included in the internal audit QA review—whether the entire function or just a separate component of internal audit, such as a separate division or geographic area.
2. Define the time period for the audits to be included in the QA review—whether from the conclusion of the last QA review or for the 12-month period prior to the announcement of the audit.
3. Determine who will be performing the QA internal audit review and ascertain that the reviewer understands both IIA standards and supporting internal audit department procedures.
4. If internal audit has not had such a quality-assurance review within the last 24 months, take steps to assure that both members of the internal audit staff and management understand the purpose and nature of the QA review.
5. If the QA review team plans to survey or interview auditees outside the internal audit department, make some preliminary plans to inform all affected persons.
6. Based on internal audits completed and in-process, develop a general strategy for the number and types of audits to be selected for review. If special knowledge areas are to be included, such as computer security or automated design, determine that appropriate resources have been allocated.
7. Decide if the QA review will be on a top-level basis, checking for compliance to general standards or planned to include detailed reviews of selected audits, including workpaper reference checks or reperformance of tests.
8. If problems are encountered in the course of the planned QA review, such as audits requiring a more detailed review, procedures should be prepared to evaluate the QA review's scope or schedule.
9. Develop a general procedure for the format and nature of the QA final audit report.
10. Develop a strategy for reporting the results of the QA review to other members of the internal audit department and to selected members of senior management.

concerns about the nature of the work performed, including the appropriateness of the audit conclusions reached and how those conclusions were communicated to management. The idea is not to determine that a representative group of auditees *like* the internal auditors who performed one or another review in their area but to assess whether the reviews were performed in an appropriately professional manner.

As a result of these review procedures and auditee surveys, the QA reviewer should summarize the results and prepare a report for the CAE. Based on these report recommendations, a plan for improvement or corrective action should be established. In some cases, if the reviewers found that certain completed audits did not follow good internal audit procedures, a program of ongoing review or corrective action should be established. If the QA review points out the need for such improvements as increased continuing education, a plan for corrective action should be established.

(c) Who Performs the Quality-Assurance Review?

Although a CAE should see the value of a QA review, an independent review party is often needed. In a large multiunit internal audit department, a team of centralized corporate internal auditors and others from different divisional units often can perform QA reviews of other divisional units. Although there is always the possibility for jealousy and nonobjective appraisals, an in-house quality review, if properly managed, can be performed inexpensively as well as effectively and efficiently. For larger internal audit departments, in-house resources can even be devoted to performing periodic quality-assurance reviews.

Many internal audit departments, however, are not large enough to perform separate QA reviews or face other challenges that prevent members of the enterprise from performing such a review. A five-person internal audit group, for example, cannot realistically conduct a QA review with one member of the staff reviewing the other four. Internal audit management has two options here. It can develop a self-assessment type of review and have all members of the staff evaluate themselves, or it can contract with an outside party to perform the review.

Outside parties that can perform QA reviews include public accounting firms, consultants who specialize in such reviews, or internal auditors from other enterprises. As another option, the IIA has a review program where it will schedule a team of volunteer professionals to perform the review. Some larger internal audit functions may find these outside approaches attractive. An internal audit self-assessment of its quality procedures can take the form of the control self-assessment (CSA) reviews discussed in Chapter 11.

A larger internal audit enterprise can perform QA reviews using designated members of the department. In many respects, an internal auditor who is familiar with the enterprise, its procedures, and the industry—and also understands general internal audit procedures—is often the best, most qualified person to review internal audit operations. Just as internal audit performs a review of another function, such as the purchasing department, the purchasing department could review itself by assigning certain people from its organization to perform this task. However, unless the purchasing department had experience performing such self-assessments, the results of the review could be viewed as self-serving. Internal audit has an advantage, as it regularly exhibits its independence through its standards and other

review activities. A larger internal audit function can perform its own effective QA reviews if it can demonstrate to others, both inside and outside of the department, that it is acting as an independent party.

Larger internal audit functions can also establish effective quality-review programs internally by assigning qualified internal auditors the responsibility of performing such reviews. The internal audit function must be large enough to allow one auditor, or a small specialized group of auditors, to perform the QA reviews separate from their normal audit activities. In a large internal audit department, there may be enough activity to justify a full-time QA function. In addition to the reviews, it could perform other activities, such as developing audit programs and procedures. This internal-review arrangement will not work if members of the regular audit staff are pulled from the normal schedule and asked to review their peers.

Although internal auditors have standards that require them to act independently, performing their own quality reviews can be viewed as either self-serving exercises or programs to criticize someone in the department. As mentioned, the reviews are best performed by an independent function within internal audit and should follow normal internal audit procedures. That is, the internal audit QA function would schedule its reviews in the same manner as internal audit plans and schedules any normal audit. If it were doing a quality review of a separate organizational unit's internal audit function, it would schedule and announce the review like any normal audit. Once the review was completed, the manager responsible for the unit reviewed would respond to the audit report as would any other auditee. Copies of the final report would go to the director of internal audit, who could take further action as necessary.

This is a particularly effective way to organize internal audit quality-assurance reviews when the audit functions are distributed throughout the enterprise. An outside quality-assurance reviewer would probably not get to all of the geographically remote units in the course of a single review. An in-house set of quality-assurance reviewers could.

Self-assessment reviews, as discussed in Chapter 11, are often the most realistic way for a very small internal audit staff, perhaps with fewer than 10 members, to review its own operations. The staff might block out time to perform the self-assessment review. Time could be allocated for this type of review when the staff was not otherwise busy with scheduled audits.

When the same internal audit staff responsible for normal audit procedures perform a self-assessment review, it almost appears as if the auditees are auditing themselves. However, this is often the only way to review the quality of internal audit procedures in a small enterprise. Budget limitations usually prevent the hiring of outsiders to perform the review, and a small audit department cannot justify the people resources. Staff members would be asked to step back and review all of the procedures performed in the course of a series of audits, including planning, workpaper documentation, audit report content, and a variety of other matters.

Rather than writing a report about itself, findings from the self-assessment review are often shared through a series of introspective review meetings. Here, internal audit management and all parties involved would take steps to improve operations based on the self-assessment review findings. For a smaller internal audit enterprise, self-assessment is usually a cost-effective way to measure quality assurance. People are often their own best critics.

31.6 Launching the Internal Audit Quality-Assurance Review

The CAE should take the lead in launching a quality review program of internal audit if a formal QA function is not already in place. It does not matter who starts the review, but the internal audit staff will recognize the significance of the CAE initiating such a process. If the outside auditors, for example, suggest such a review to members of the audit committee, all parties will wonder what is wrong with internal audit. But if internal audit itself initiates the process, it will have much greater flexibility to suggest the most appropriate parties to perform the review. When an enterprise's external auditors propose an internal audit QA review, the implication is that they will probably be contracted to do the work.

Internal audit may initiate its own quality review as part of the internal audit annual budgeting and planning process. A basic audit program can be developed and resources allocated for either creating a separate QA review function in the enterprise or contracting the review process to an outside provider. A quality review process should not be considered a one-time event; it should be a continuing mechanism to assess the quality of overall internal audit performance.

When a CAE proposes a program of internal audit quality-assurance reviews to the audit committee and senior management, he or she may be subject to a number of questions.

If the work is planned to be performed by a specialized in-house group, for example, the CAE may be asked why existing internal audit staff cannot be pulled off other audit work to perform the reviews themselves. The CAE needs to emphasize the importance of performing these reviews independently and in a manner that will not limit other planned audit activities. If the review is to be performed by an outside consulting firm specializing in such reviews, the CAE should document why it would be preferable to use outside auditors. In either case, the CAE may find that some selling is involved to convince management of the need for the reviews and the approach to be used.

Management will readily accept an internal audit QA review process if internal audit presents a good plan to perform these reviews on an ongoing basis, if the reviews will allow auditees to provide input regarding their impressions of the overall internal audit process, and if the QA review process points to an improved internal audit function in the enterprise. In addition to selling management on the need for such a QA function, internal audit management should inform all of the internal audit staff of the plans to perform the function. Care should always be taken to emphasize that the reviews are not intended to be a witch hunt but are designed to improve the overall quality of all audits performed. Properly explained, the process should be enthusiastically accepted by members of the internal audit staff.

Although an overall plan for performing QA reviews over a period of time is needed, established procedures are necessary to any perform a single, comprehensive review of an internal audit function. The necessary steps are to establish the objectives of a given review, to understand internal audit staff procedures, to survey or interview a selected group of auditees, and to report the results of the review to management and other interested parties. The QA review process often is performed by a specialized, independent group within the internal audit. Self-assessment reviews where members of internal audit perform reviews of their own audit activities are particularly appropriate for a smaller enterprise.

(a) Quality-Assurance Review Approaches

An internal audit function launching a QA review program needs to make some basic planning and organization-level decisions. In addition to deciding who will be performing the reviews, internal audit management must decide on the scope, depth, and breadth of the reviews to be performed. *Scope* here implies the amount of detail to be included in any review. Should the review include primarily internal audit administrative procedures, or should it extend to detailed reviews of such areas as IT audit practices or audit sampling approaches? *Depth* here refers to the amount of detail to be included in the QA review of any area. With an extended scope, the QA reviews might delve into the detailed audit procedures performed in each audit reviewed. It is one matter to determine that a selected audit project to be reviewed has a planning memo, a set of workpapers, and an audit report on file. In an extended scope review, the QA reviewers might examine the detailed audit procedures performed for each audit selected. This might include a detailed review of workpapers and even the reperformance of some tests. *Breadth,* as used here, refers to the number of units to be included in any QA review. Should the QA review be restricted to the larger centralized audit function at headquarters, or should it extend to remote units? In other enterprises, the geographically remote units may be subject to QA reviews but headquarters will not. In other instances, internal audit management will review domestic units and not go overseas or will review one operating division but not others. Auditees may or may not be surveyed depending on the review approach selected.

Decisions should be made as to the frequency of planned QA reviews. In a large, geographically disbursed enterprise, a QA function will probably not be able to review every internal audit unit every year. The selection of whom to review—and how often—should depend on the criticality of the internal audit function reviewed. The same risk-assessment techniques introduced in Chapter 6 can be useful in helping internal audit management decide which areas are to be included as part of annual QA review plans. If a given area was subject to an earlier QA review and areas in need of corrective action were identified, the QA review function may want to schedule an additional follow-up review in that area. Even if an outside consultant perform QA reviews, internal audit management should take a major role in deciding on the scope, depth, and breadth of the reviews to be performed by the QA reviewers over a specified time period (often one year). Internal audit management should take the lead in specifying the types of reviews to be performed as well as the expected outputs from those reviews. Sometimes outside reviewers tend to work according to their own agenda. The CAE should be responsible for outlining this QA review approach subject to risk-analysis studies and various other inputs from enterprise management.

While these comments have assumed that the CAE will have a strong input into the QA review process, the CAE's role in administering and reviewing internal audits is also within the scope of any review of overall QA procedures. For example, if internal audit standards call for the CAE to sign the engagement memo and if the CAE ignores this duty, the QA review should highlight this discrepancy. This scope allows the review to assess the overall quality of performance by the entire internal audit function.

The CAE should emphasize to the quality team performing the work that it has an obligation to assess the overall quality of the internal audit function. Once the

EXHIBIT 31.8 Quality Review Engagement Letter Memo

Corporate Internal Audit

Global Computer Products

To: XYZ Division Internal Audit Staff
From: Tom Goodguy, Quality Assurance Manager
Subject: Quality-Assurance Review

As part of our established internal audit procedures, the internal audit Q/A department periodically selects areas for review to assess compliance with department and general internal audit standards. Since we have not performed a review in your area for over two years, the XYZ Division internal audit function has been selected for a quality assurance review starting May XX, 20YY. I will be directly managing this review and will be assisted by two staff members.

Please send me a current schedule for internal audits completed over the past year as well as a copy of your current annual audit plan. We will select two audits completed over this period and will request to see the workpapers in advance.

We plan to arrive at the XYZ Division internal audit office on the morning of May XY and would like to meet with your team at that time. We expect that our fieldwork will require no more than two weeks, at which time we will arrange to meet with the XYZ Division Internal Audit team to discuss our initial findings and recommendations.

Thank you for your cooperation and please contact me if you have any questions.

Tom Goodguy

reviews have been selected, the approach established, and a plan developed, senior internal audit management should inform all members of the internal audit function of these QA review plans. For a larger internal audit function with multiple units, that communication could take the form of a formal memo announcing the review plans and the need for cooperation. A sample memo is shown as Exhibit 31.8. A similar note should be directed to auditee groups that may be asked to participate in interviews or surveys. All parties need to be informed of the objectives of the QA review program. Even if internal audit has an ongoing review program, a notice similar to Exhibit 31.8 will remind internal audit team members that this review program is starting another new, often annual cycle.

(b) Example Quality-Assurance Review of an Internal Audit Function

This section describes how an internal audit QA review might be performed by internal auditors using an example company. The review covers the internal audit department at Axylotl Specialties, a separate, semi-independent division of the enterprise. Axylotl Specialties is 75% owned by the headquarters company, with the remaining 25% held by outside investors. Assume Axylotl Specialties' internal audit function ultimately reports to the headquarters' CAE but does not have day-to-day audit project-related contact with the headquarters' audit staff. As with many decentralized enterprises, the internal audit function of the Axylotl Specialties has been

asked to follow general guidance from headquarters but has the freedom to establish some of its own local procedures based on the unique audit risks found in its business. In addition, Axylotl Specialties has its own audit committee.

This QA example review follows the general procedures outlined in Exhibit 31.7 and assumes that the headquarters' review team has had little contact with Axylotl Specialties. While this example assumes that the group to be reviewed is an independent unit of the parent corporation, these same basic procedures can be used by a variety of different reviewers and for various internal audit units.

(i) **QA REVIEW PRELIMINARY PLANNING** The internal audit QA review team should follow some of the same procedures that it would use when performing a normal internal audit. These might include:

- **Announce the planned QA review.** The review should be announced to all members of the internal audit staff who might be impacted. Members of the internal audit staff might be offended if they do not know about the planned review and its objectives. The review announcement should contain a strong message that the purpose of the review is not to get anyone on the internal audit staff but to help the overall internal audit enterprise to become more efficient and effective.
- **Assign resources to perform the review.** Concurrent with or even prior to announcing the review, decisions need to be made regarding who is to perform the work. If performed by an outside provider, objectives and review schedules should be defined. An internal audit QA review should have designated persons who will be performing the work and who will not be distracted by other projects.
- **Meet with internal audit management.** In a larger internal audit group, the CAE is often responsible for initiating the review by scheduling it with the specialized function within internal audit that will perform the work or by contracting with an outside provider. Other members of the internal audit management team may not have that much knowledge about the planned review. Before starting the actual work, the review team should meet with appropriate members of audit management to advise them of its review approach and to discuss any special considerations that might impact them. For example, the QA team may schedule a review at a separate, divisional internal audit function. Local internal audit management, however, may suggest that the reviewers not look at one or another area. If the request seems reasonable, the QA team should honor it and document that decision.
- **Meet with other members of management.** Enterprise management is normally quite aware of their internal auditors' work products through their reviews in various operational areas or through audit reports, but they may not be aware of the objectives of an internal QA review. The review team leaders should meet with members of local management to explain their review objectives. The review team should also request some input from management regarding any of their concerns about the performance of internal audit. For example, management may feel that certain audit reports took far too long to issue or that some members of the audit enterprise have not been acting in a professional manner. This type of input may point the review team to examine completion times for the audits mentioned or to review training records for the audit staff.

After completing these first steps, the QA team should be ready to perform the actual review. Assuming that it has established a starting audit program, it may want to modify the scope and extent of its planned review based on these inputs. If a branch unit audit manager has indicated that a very critical audit will be in process when the review is scheduled, the review team may want to reschedule its review of that area.

(ii) QA INTERNAL AUDIT REVIEW PROCEDURES An internal audit QA review is an independent assessment of the audit department's performance in compliance with internal audit professional and departmental standards. No single approach applies to all internal audit departments and all reviews. Generally, a review will investigate internal audit office procedures and enterprise standards and then focus on individual completed audits to determine if the standards have been followed. Exhibit 31.9 describes some of the major review steps for a QA review of internal audit operations. The reviewers here need to understand specific internal audit departmental procedures. This requires an initial study of documentation and other materials as a first step, just as internal auditors would review available documentation as a first step in operational audits. Even if members of the same overall audit enterprise are performing the QA review, the review team should still review the internal audit documentation prepared by internal audit in past reviews. It will reacquaint them with operations and will allow them to better define their audit tests. This documentation standards review may also point to additional areas to emphasize in their detailed testing procedures. For example, the reviews may find that internal audit's standards for auditor project timekeeping are extremely complex. Too complex requirements may suggest that internal auditors have trouble completing the time reporting and may not be keeping accurate time records. This might point to an area for more detailed review.

Items reviewed within the internal audit department should be selected on a test basis. While audit item selection here might not be an appropriate area to perform detailed statistical sampling test selection approaches, the review team should use judgmental sampling in the various areas reviewed. That is, internal audit might not care to reach an attributes sampling type of conclusion, as discussed in Chapter 9; however, the review team should take care to make representative selections of all areas sampled. For example, if the QA reviewers are interested in whether internal audit has been performing an adequate risk analysis in various areas of the enterprise, the review team might judgmentally select several areas of overall enterprise operations and determine if an adequate risk analysis had been performed in those areas.

The actual QA review procedures to be performed are essentially the same as for all other audit procedures described throughout this book. The reviewers should identify an area from their established review program, select a representative sample of actual items in that area, review or test the items selected, evaluate the tests, and document the results. The QA review team should take the same care in selecting and documenting its work as it would expect internal audit to follow in its regular audits. As with normal internal audits, when the review team finds what appear to be significant exceptions, it should discuss these potential findings with the internal auditors being reviewed to determine if there are extenuating circumstances behind the potential findings. This is the same process followed in any internal audit, except that here the reviewers are auditing the auditors.

EXHIBIT 31.9 Review Steps for a Quality Assurance Review of Internal Audit

1. Review internal audit department approved procedures to determine if adequate emphasis is devoted to accuracy and quality issues; summarize any areas for potential improvements.
2. Review the current and most recent past year of the completed audit plan:
   a. Assess reasons for any audits never launched or still in progress.
   b. Review the hours recorded for completed audits and compare to original plans; determine and document reasons for any major plan variances.
   c. Review the extent of special, unplanned audits performed and assess both their supporting documentation and reasonableness.
3. For the current period and the past two years, review the risk analysis and audit planning process. Assess whether appropriate attention was given to relative risks in all scheduled audits.
4. Select a sample of audits completed over past two years and review their complete workpapers to ascertain:
   a. Workpapers are in good order and follow internal audit department standards for both hard- and soft-copy formats.
   b. Audit programs were developed for each review that support audit scope, identified risks, and work performed.
   c. All potential findings have either been carried to the audit report or have otherwise been resolved through appropriate disposition.
   d. Appropriate audit reports or other communications were prepared following good internal audit standards.
   e. All audit documentation reviewed in controlled in secure repositories.
5. Based on the workpapers and other supporting materials reviewed, assess internal audit's use of CATTs, audit sampling, and other audit techniques.
6. Interview key auditees from several of the selected audits completed to assess their impressions of both the professionalism of the assigned internal audit team and the results of the audit work.
7. Review overall internal auditing budgeting, travel expense, and time reporting procedures to determine their reasonableness and thoroughness.
8. Review the time budgets prepared for the selected review audits and compare them with the actual hours required for the selected reviews; review any documentation covering major differences.
9. Review the internal audit continuing education activities to determine appropriate attention is given to professional training.
10. Review internal audit staff turnover and assess potential causes for any high turnover.

(iii) REVIEWS OF INDIVIDUAL COMPLETED AUDITS In addition to an assessment of overall audit group procedures, a QA audit should always include detailed reviews of a sample of completed audits. This audit review should not be made to second-guess the findings of the staff auditors who performed the work but to determine that the selected items followed good internal audit standards throughout, including planning, test procedures performed, workpaper documentation, and the completed audit report. The steps described previously reviewed internal audit department standards; this phase of a QA review assesses compliance with the standards in the completion of actual audits.

Normally, a QA review team should select a representative sample of materials from completed audits over perhaps the past one-year period. This sample should

include all types of audits, including operational, financial, IT, and other types of special reviews. A good starting point here is to look at an audit project report listing completed audits. From this, the review team should select its sample and pull the workpaper files and any other related data to describe the audit procedures performed, the conclusions reached, and the method for communicating those audit conclusions. The reviewers should read enough of the workpapers to understand the audit objectives, the approaches used, and the conclusions reached. If the material reviewed has what appears to be a good process where audit supervisors or others review all workpapers and appear to ask appropriate questions prior to the completion of normal audits, the QA review team can conclude that the process is working for all of the audits selected.

QA should determine if departmental procedures are being followed and if good auditing practices are used. The number and extent of areas that might be included in such a review will vary with the overall type and scope of the audit. They might include:

- **Audit sampling procedures used.** Chapter 9 discussed audit testing procedures, including the use of statistical and nonstatistical sampling procedures. The internal auditors who did the actual work may have made a decision to only pull a limited judgmental sample when a better audit result might have resulted from the use of some type of statistical sampling approach. An appropriate QA comment is that the auditor in charge of the review did not appear to have considered the better results that might have been gained from statistical sampling techniques.
- **Compliance with generally accepted accounting principles (GAAP) or other accounting standards.** While internal auditors will generally not be performing financial audits, many audits have some financial accounting ramifications. In many cases, these reviews may have been performed for the external auditors who would be responsible for reviewing the work and signing off on the conclusions. However, if the financial accounting procedures performed were strictly part of internal audit's review, the QA reviewer might want to consider the appropriateness of the financial accounting procedures as documented in the workpapers.
- **Appropriate consideration of IT risks.** Operational audits sometimes do not consider the IT risks associated with the area reviewed. For example, an operational or financial review might rely on the outputs of an IT system, with no attention given to the controls surrounding that system. An appropriate QA review point is to comment on the assessment of IT risks.
- **Use of computer-assisted audit tools and techniques (CATTs).** Chapter 21 discussed the use of CATTs to introduce efficiencies into the process of gathering audit evidence. If the audit workpapers reviewed do not evidence the use of these techniques, this may be an area for a review comment.
- **Use of other audit automation techniques.** Chapter 16 discussed the preparation of workpapers to document audit activities. While many of the areas discussed there are not appropriate for a QA review, the chapter emphasized some automated techniques that could be used to make the audit and workpaper-preparation process more efficient. Again, this is an area for potential QA review and comment.

These are just a few examples of the many areas that might be included in a QA review of completed workpapers. In some instances, the QA reviewers may want to discuss the work with the internal auditors who completed the review and prepared the workpapers. Although the audit workpapers should speak for themselves, the internal auditors who did the work often can provide additional background information. A need to ask specific questions about audit procedures not documented in the workpapers may point to lack of documentation; however, these questions are sometimes necessary for clarification purposes. Also, the QA reviewers often will want to interview or survey the actual auditees.

The actual audit report and its findings are also part of the QA review of the completed audit workpapers. The reviewers should determine that all points covered in the workpapers and identified as potential report findings have been included in the final audit report or have otherwise been properly disposed of. The QA review should not focus on style and small grammatical errors; it should assess whether the report has been clearly written and is in accordance with internal audit department standards. The reviewers may want to consider the elapsed time between fieldwork completion and report release. Too long of a delay in report production may indicate some overall internal audit quality problems. The review of workpapers should include all of the steps documented in the internal audit process, from risk assessment and initial audit planning to the release of the final report, including auditee responses.

(iv) AUDITEE INTERVIEWS AND SURVEYS A QA review should include interviews or surveys with a sample of internal audit service recipients. The internal audit QA reviewers may want to select a sample of recent internal audits and interview both the auditees and the recipients of the issued reports from those audits. The QA reviewers should contact members of enterprise management to better understand their impression of internal audit's services. These surveys with persons outside of the internal audit department can provide different perspectives on the audit work performed and may point to different potential conclusions regarding internal audit services.

Benchmarking is a different type of internal audit survey where reviewers interview persons from audit departments in other enterprises. The idea here is not to assess how the entire internal audit department stacks up with similar internal audit functions in other enterprises. This type of exercise is most meaningful when data are gathered from an internal audit group of a similar size and in a similar industry. Some internal audit benchmarking is often done on a CAE level through informal professional contacts; QA-sponsored internal audit benchmarking formalizes this process and provides a better understanding of what internal audit departments in other enterprises are doing. The benchmarking process is discussed in Chapter 11.

(A) Quality-Assurance Auditee Interviews. After reviewing workpapers and other materials from a completed audit, the QA reviewers usually find it valuable to interview some of the auditees. (These are the persons whose functions were reviewed as part of the completed audit selected for the review.) The idea here is to assess the level of internal audit professionalism as seen through the eyes of the auditees. Even though the QA team may have found the selected workpapers to be well organized and the audit report well written, internal audit has a potential quality problem if

the auditees—the subjects of the audit—did not regard the internal auditors who performed the review as high-quality professionals.

Many factors can cause this type of feeling. For example, perhaps the field audit team worked late into the evening one day but arrived at the audit site late the next day. Because auditees do not know that the team worked late, they might resent and comment on the auditors' work habits. QA interviews with selected auditees might reveal this type of information.

Auditee interviews are usually initiated following a QA workpaper review. While not every auditee identified in the workpapers should be contacted, the review team might consider asking a small sample of these persons to participate in an interview. Even though QA may want to talk to several auditees identified in a single set of workpapers, all QA interviews should involve only one auditee at a time. This one-on-one approach allows an auditee to be more open in expressing concerns regarding an audit.

Although QA auditee interviews can provide much information about the quality of the internal auditors performing a review, they also can present difficulties. First, an auditee may not respond honestly to the interviewer's questions. The auditee may not want to hurt the members of the audit team and may be reluctant to express honest opinions. Even worse, if a group of auditees are interviewed together as a focus group, the session may transform into a "feeding frenzy" where a large amount of negative but unsupported bad news is communicated.

Exhibit 31.10 outlines the types of questions a team of QA reviewers might ask selected auditees. The interviewer should clearly state that the purpose of the review is to measure the overall quality of the audit procedures performed and not to get anyone. The auditee being interviewed should be assured that all responses will be kept confidential—similar to the procedures followed in a normal audit. If appropriate, the interview responses should be summarized to capture total auditee impressions regarding the review.

(B) Internal Audit Quality-Assurance Surveys. Interviews, as discussed, are generally limited to a small group of auditees involved with only a limited number of selected internal audits. In some instances, the QA review may find some value in surveying all auditees in a given division, department, or larger business unit that has had contact with internal audit. This approach usually works best when QA is reviewing the internal audit function in some geographically remote unit, where the review team has little knowledge of local internal audit operations. The survey might be mailed out prior to the arrival of the QA team, with instructions to mail back the responses. If done in advance, the internal audit QA team may be able to identify some potential concerns before the initiation of the actual QA review. The QA team conducting the survey should carefully classify the survey data to identify trends or issues.

(c) Reporting the Results of an Internal Audit Quality-Assurance Review

An internal audit QA review, as we have discussed, is an internal audit review of internal audit. Thus, a QA review should follow many of internal audit's normal procedures, including planning, fieldwork, documentation of results, and issuing the audit report. A QA review is of little value unless its results are reported to the audit committee and others in a formal audit report. Depending on the size of the

EXHIBIT 31.10 Quality-Assurance Auditee Review Questions

As part of our effort to maintain the highest level of professionalism, we are asking you to help review our performance in a recent audit performed in your department. We are interested in the _____ audit that took place between mm/dd/yy and mm/dd/yy and was led by _____.

Please take a few minutes to answer the following questions. If necessary use additional sheets and send your response in the enclosed envelope.

1. Did you understand the purpose and objective of the audit? Did you receive a formal letter announcing the audit?
2. Did the audit start when it was planned and finish as you expected?
3. Did the internal audit team maintain a professional attitude consistent with your department, in terms of such matters as their work hours, dress, and attention to work during the day?
4. Did the audit team appear to understand the area they were reviewing? Did they ask questions when appropriate? Did those questions appear excessive?
5. Was the audit performed so as not to hinder your normal work activities?
6. Were matters of audit concern, particularly those that were included in the final audit report, discussed with you in the course of the review?
7. Did the audit conclude with a formal exit meeting? Were the auditors' matters of concern discussed with you and did you have an opportunity to respond as appropriate and to provide additional data when necessary?
8. Was the audit report for the review delivered in a timely manner and did it reflect the final closing meeting and any additional clarifications that you may have added?
9. Were the audit recommendations in the final report appropriate and helpful?
10. In general, what was your overall opinion of the audit?

internal audit department and the scope of the QA review, the completed review might follow a normal internal audit report, as discussed in Chapter 17. That is, the QA reviewers should prepare a draft report with their QA review findings. The audit group reviewed then has an opportunity to respond to those findings, outlining the corrective action steps they plan to take, The final product would be a QA report similar to a regular internal audit report.

A key difference between an internal audit QA report and a normal internal audit report, however, is the report distribution. This QA report is normally addressed to the CAE with copies to the audit committee; few if any other persons outside of internal audit are on the distribution list. The report may cover some very specific and technical details of problem areas identified by the QA team and thus may go into far greater detail than should be included in a well-drafted internal audit report. The QA review team is responsible for discussing areas where the internal audit area reviewed can improve its procedures; internal audit itself is responsible for making certain that appropriate corrective actions are taken. The CAE is normally responsible for deciding if persons outside of internal audit should receive a copy of the internal audit QA report. The CAE is responsible for determining that all aspects of the internal audit department follow good practices and that any appropriate corrective actions are taken.

A smaller internal audit department or an enterprise that has not devoted formal resources to performing formal QA reviews should still take steps to monitor the

quality of its internal audit activities. This quality review can be performed through self-assessment surveys, which can take many forms, ranging from an open discussion in response to a How are we doing? type of question raised at a departmental session, through the completion of a formal self-assessment review or questionnaire. While an open discussion will give the CAE some information on how well the small audit department is doing, a self-assessment survey is most useful.

The idea is to ask all members of the internal audit department to complete a survey where they will respond to questions regarding their audit practices and how well they think that they, the individual auditors, as well as the department as a whole, are doing. Despite the size of the department, all members of the team can evaluate how they feel they are performing as individuals and as a team on their audit assignments, and how the overall audit department is performing in the eyes of each individual auditor. Each member of the audit department completes a survey, tailored to the individual internal audit department, which emphasizes compliance with internal audit standards and the overall perceived quality of the work performed. A limited number of users of internal audit services might also be polled through this type of survey.

A small internal audit enterprise may be faced with the question of who should complete the survey. If the department consists of the CAE and perhaps only a staff of six, that director would know which of the internal audit staff completed the surveys based on the nature of some criticisms or even handwriting. In such cases, these surveys should be run independently. The CAE might ask the human resource department to mail out the surveys and to compile the mailed-in results. This way, the survey responses would not be easily connected with the persons completing them, and staff members would feel freer to express their honest opinions.

Once the survey results have been tabulated by the responsible nonaudit party, the CAE should share them with the audit staff. Although this type of assessment will not result in a formal findings and response type of audit report, members of the audit staff can collectively decide on various areas for improvement and should take steps to change operations as appropriate. While it is not as comprehensive as a formal internal audit QA review, an independent self-assessment review is a good exercise for smaller internal audit departments to evaluate their performance.

31.7 Future Directions for Quality-Assurance Auditing

This chapter has looked at quality assurance from two different dimensions: the separate quality audits that were the domain of the ASQ quality auditors and QA reviews to assess the standards and performance of existing internal audit departments. While QA standards and practices are important for all internal auditors, we can at some time lose track of our objectives in this area because too many use the term *quality assurance* without fully understanding this process.

This chapter began with a discussion of the role of ASQ members who once called themselves quality auditors, not just auditors. They are important members of the overall internal audit community, but because of their manufacturing and process industry heritage, they often operate separate from conventional internal audit functions and sometimes have only minimal contact with the CAE and audit committee. We have called this group quality auditors to distinguish them from the IIA-heritage internal auditors. Even though their IIA and ASQ professional organizations do not

have any formal connections, we can expect these two audit professions to grow closer in the future. IIA-trained internal auditors need to learn and use some of the analytical and statistical tools that are common to ASQ quality auditors, and quality auditors need some of the rigor and discipline of the IIA's internal auditors.

Internal audit QA reviews are methods that allow an internal audit department to measure how well it is performing. Internal auditors perform reviews in many other areas and freely make constructive suggestions, but often they do not take the opportunity to review themselves. A formal program of internal audit QA reviews will allow internal audit to better assess its own performance with reviews performed by a specialized function within internal audit, by qualified outsider reviewers, or by a self-assessment survey. Who performs the review will depend on the size and activities of an enterprise's internal audit department as well as on management's commitment to this type of review program.

In addition to reviewing how an individual internal audit department is doing and how well it is complying with internal audit standards, an internal audit department often needs to assess how it is performing compared to internal audit functions in other enterprises. This is where the concept of benchmarking is useful. An internal audit QA function can meet with other internal audit groups and determine how those groups are performing. Similarly, the well-run internal audit function should share its ideas and practices with other internal audit functions that are doing their own benchmarking. This becomes even more important with the IIA standards requirement that every internal audit function must arrange to have an external quality assurance review at least once every five years. Understanding these internal audit QA requirements and the steps necessary to perform an effective QA review is an important internal audit CBOK requirement.

Notes

1. ISO CD2/ISO 19011 (Milwaukee: ASQ Quality Press, 2000).
2. SAS No. 70 is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants, officially titled "Reports on the Processing of Transactions by Service Organizations." It defines the professional standards used by a service auditor to assess the internal controls of a service organization and issue a service auditor's report. Service organizations are typically entities that provide outsourcing services that impact the control environment of their customers. Examples of service organizations are insurance and medical claims processors, trust companies, hosted data centers, application service providers, managed security providers, credit processing organizations, and clearinghouses.

CHAPTER 32

Six Sigma and Lean Techniques

Enterprise operations managers, at all levels, are regularly looking for ways to improve their operations, whether in shop-floor production processes or for office administrative procedures. Internal auditors have a major role here through their internal controls reviews and audit report recommended corrective actions. As discussed in Chapter 28, they can also have a strong role in process improvements by serving as internal consultants to their enterprise. There is no single solution or methodology for implementing best practices to improve operations, and many different approaches have been tried over the years. Some are still in use while others are but footnotes in business history.

An overall quality improvement approach called six sigma was first based on Japanese quality assurance techniques and has now been used successfully in the United States and throughout the world to reduce errors and improve efficiencies in all aspects of enterprise operations. Six sigma has its roots in statistical quality control procedures but is now viewed as much more of a process improvement approach. However, because of its roots in Japanese quality manufacturing processes, knowledgeable practitioners are designated as green belt certified (using Japanese karate terminology); experts are certified as black belts. Adoption of a six sigma approach can become an almost all-consuming exercise for many in operations.

Chapter 31 discussed quality assurance processes and the role of the American Society for Quality (ASQ) quality auditors. While those quality auditors normally have some understanding of the six sigma concepts that are the topic of this chapter, all internal auditors—IIA as well as quality auditors—should have a basic common body of knowledge (CBOK) understanding of six sigma concepts and how they are applied.

This chapter provides a high-level introduction to six sigma concepts and how they should be applied in many aspects of enterprise operations. We provide an overview of six sigma as well as some lean approaches to implementing it. *Lean* is an expression that is increasingly used in business procedures today. It is an approach that takes a comprehensive but very document-oriented process and breaks things down to essential bare minimums. A concept that is useful in many areas of operations, the lean technique is particularly valuable for understanding the important aspects of six sigma operations.

Even though an internal audit function may not be using six sigma concepts as part of its overall operations, all internal auditors should have a basic CBOK understanding of this important quality improvement concept. An internal auditor will encounter auditees in all levels of operations who may talk about their six sigma achievements and activities. The professional internal auditor should have sufficient

background information to understand six sigma concepts and to ask important review questions.

32.1 Six Sigma Background and Concepts

Most internal auditors will recognize "sigma" as one of the letters of the Greek alphabet. As a capital letter, sigma appears as Σ. In mathematics, this symbol normally refers to the sum of a series of numbers following it. In its lowercase form, sigma appears as σ. Here it is used to express the variability from some process. For example, Chapter 9 on audit sampling described how variable data are often organized in a bell-shape curve, a standard distribution illustrated in Exhibit 9.5. The σ or sigma symbol is used to describe the variability around the central points or averages in a standard distribution.

Enterprises have used these σ-based variability measures to measure product or process quality. For example, enterprises traditionally accepted quality measures of 3 or 4 sigma level as a norm. That is, they would accept error or problem levels of between 6,200 and 67,000 problems per million opportunities. We can think of these measures in terms of some part rolling off a highly automated production line. Whether in the United States or elsewhere in the world, enterprises would accept that level of problems with these high-volume production parts, assuming they could fix or repair things later.

This concept of an acceptable level of quality changed in the 1970s when a Japanese company took over production processing for what had been a Motorola production plant producing Quasar-brand television sets. The Japanese company installed its own production and quality procedures and was soon producing products with only 1/20th of the defects that Motorola production management had tolerated. The Japanese company was operating at six sigma.

Motorola enthusiastically implemented these six sigma quality standards throughout its production and other operations. It became a recognized leader in quality operations, and the company received the U.S. government's Malcolm Baldridge National Quality Award in 1988. Many other major companies, such as General Electric and Allied Signal, also embraced six sigma concepts as an approach to improve customer service and productivity. Six sigma remains an important process improvement process today.

Although six sigma began as a statistical quality assurance concept, its real importance is its use as a program to improve overall process quality, whether in manufactured products or in service-related processes. The chief executive officer (CEO) does not announce implementation of six sigma at a major meeting with little action taken beyond those broad statements. Rather, an effective six sigma initiative is implemented through the efforts of small teams using what is called a design-measure-analyze-improve-control (DMAIC) model, consisting of these steps:

- **Defin** the goals for the improvement activity.
- **Measure** the activity covering the existing system.
- **Analyze** the need to identify ways to eliminate gaps between the current performance of the system and the desired goal.
- **Improve** the system initiatives.
- **Control** the new or revised system.

These DMAIC steps define the overall philosophy behind six sigma. Although it got started as a precise—many decimal points—quality and process improvement process, six sigma today is much more about the steps necessary to improve enterprise processes. These steps include observing existing processes of all types and levels, developing a hypothesis to potentially improve the observed operation, then making predictions to improve the area of concern. A designated six sigma team then installs the suggested changes, tests the results of those changes, and repeat these steps as necessary to make effective improvements.

Internal auditors should recognize some very strong differences between a six sigma–led team and their typical auditee environments. Internal auditors generally review operations in an area and make recommendations for improvement through published audit reports. Internal auditor recommendations are based on their experiences as well as suggested approaches that may be developed through discussions before the release of the published audit report. These are not flexible or best-guess recommendations, and it may be a long time before internal audit returns to see if those internal audit recommendations have been implemented.

Six sigma process improvements do not come from outsiders—such as internal auditors or consultants—visiting an operation and then making tentative suggestions to improve processes. Rather, a team of trained specialists in an area of operations reviews operations and implements process improvements throughout their own area of operations. There are opportunities here for internal auditors on three levels.

1. When the internal audit team discovers a six sigma process in place during a scheduled audit, following its service-to-management objectives, the on-site audit team might expand its audit procedures and consider reviewing the effectiveness of the six sigma program.
2. Internal auditors may want to consider recommending six sigma processes as part of their reviews of internal controls in some area.
3. Internal auditors should consider the use of six sigma processes to improve their own internal audit operations.

All of these opportunities, of course, require that an internal audit team have a CBOK general understanding of six sigma processes. While quality assurance auditors (discussed in Chapter 31) are usually very well aware of six sigma, many IIA-heritage internal auditors today have not been exposed to these important concepts. As of mid-2008, for example, a search on the IIA Web site home page for "six sigma" returns a blank. This chapter provides a high-level overview of six sigma for internal auditors. A general understanding of six sigma processes should be part of every internal auditor's CBOK.

32.2 Implementing Six Sigma

The concept of six sigma calls for an enterprise to implement improved processes that will allow delivery of no more than 3.4 defects per million opportunities (DPMO) for a production product or process step. Although we are using the term *six sigma* throughout this chapter, today it is often referred to as 6σ in professional documents. At first glace, six sigma sounds like a very tough standard to meet. However, thousands of companies have successfully implemented six sigma programs. In most

cases, the effort has been launched by a fairly senior manager who has acted as a catalyst for improving service quality. The whole idea is less about statistical-led quality management than establishing a new initiative throughout the enterprise. For many, six sigma develops in a manner similar to how family members might convert to a new religion. One family member is exposed to the new religious philosophy, takes some additional training, and then brings in "experts" from the new religion to teach and convert other family members. They then subscribe to the new philosophy, establish goals, and continue to actively follow and work under that new religion.

Our family religion conversion analogy is weak because religion deals with intangible benefits. Six sigma calls for an enterprise to establish some very definite goals that will begin to provide benefits once deployed. Exhibit 32.1 outlines the types of deployment and process goals an enterprise might attempt to achieve by adopting a six sigma program.

EXHIBIT 32.1 Six Sigma Deployment and Process Guide

- Identify goals to enhance business needs.
  - Increase shareholder value.
  - Increase revenues, returns on investment (ROI) and profitability.
  - Improve market share.
- Operations level goals.
  - Reduce material and labor costs.
  - Eliminate production rework at all levels.
  - Improve production and process throughput.
- Process level goals.
  - Improve cycle times.
  - Reduce process resource requirements.
  - Improve process yield through reduction in defects.
  - Reduce all levels of variability and improve process capability.
- Identify deployment goals of operations value streams.
  - Define the processes that are critical to enterprise performance.
  - Analyze how key processes bring value to customers.
- Determine metrics and current performance levels.
  - Develop techniques to measure key value streams.
  - Identify processes that are stable and subject to statistical control.
  - Establish process measures, such as cycle times, costs, and quality opportunities.
  - Define process should-be objectives where appropriate.
  - Define benchmark or best-in-class performance measures.
- Establish breakthrough strategies for new performance levels.
  - Identify the variables that make the most differences to process performance, and establish settings or goals for them.
  - Identify areas where processes can be designed to become more robust.
  - Define areas where process redesign will yield production of quality improvements.
- Standardize new production or process approaches.
  - Develop and release operational procedures covering new approaches.
  - Train people, as necessary, to use new approaches.
  - When necessary, implement statistical measures to control process variation.
  - Modify inventory, accounting, and other business systems to ensure the improved process performance is reflected in overall operations.

(a) Six Sigma Leadership Roles and Responsibilities

An effective implementation of six sigma in an enterprise requires designated leadership and a strong, trained team of employees. Six sigma projects are normally launched in addition to typical job responsibilities. As mentioned, six sigma introduces a series of new professional certifications based on its Japanese heritage. While there are special training responsibilities for each, an enterprise leadership team to launch and manage six sigma should include:

- **Six sigma executive council.** A top-level group of senior managers across the enterprise should be formed to manage the initiative. This group suggests and approves high-impact six sigma projects, tracks progress, reviews the effectiveness of the program, and generally act as a conduit for six sigma communications throughout the enterprise. The executive council is like an audit committee for a six sigma initiative.
- **Six sigma director.** This person directs and manages all six sigma efforts. The director is the six sigma program manager for multiple six sigma projects and leads overall deployment efforts. The director leads and evaluates the overall initiative and communicates progress to customers, suppliers, and the enterprise.
- **Master black belt.** Often this is the one full-time person directly committed to leading a six sigma initiative. Certified six sigma black belts (CSSBBs) are persons who have displayed proven knowledge and expertise in implementing six sigma. This involves both "textbook" knowledge of the subject matter (methodologies, tools, principles, and related topics such as leadership and change management), as well as real-world, successful application of the methodology and tools with experience in more than one six sigma project.

  An individual can become a certified CSSBB in a variety of ways: from a professional organization, such as the ASQ; from some consulting companies; or from a six sigma active company (e.g., General Electric, Motorola, etc.). No one way is necessarily better than another, but it is widely recognized that private companies with mature six sigma programs serve as the best vehicles for certification.
- **Six sigma black belts.** These are the six sigma experts in an enterprise. Black belts lead overall process improvement efforts and take direct responsibility for specific key six sigma projects. A black belt should have a demonstrated understanding of the black belt body of knowledge, as shown in Exhibit 32.2, and a proficiency in achieving the results of six sigma approaches. Black belts frequently serve their organizations for assignments lasting one or two years, then return to their regular job duties.
- **Green belts.** These professionals have a basic understanding of six sigma processes and serve as part-time assistants to their enterprises while maintaining normal job responsibilities. They work on six sigma projects but in a more junior level than black belts.
- **Six sigma improvement teams.** Following the leadership of black and green belts, many other persons may be assigned to a six sigma project on a part-time basis. Depending on the nature of the project, there may be a need for detailed data gathering, process testing, or preparation of documentation to achieve six sigma results.

High-Level Six Sigma Understandings
☐ Overview of six sigma and its language
☐ DMAIC methodology overview
☐ Financial benefits of six sigma
☐ Understanding the impact of six sigma to the enterprise
Define Six Sigma Elements
☐ Project management
☐ Project definition
☐ Project charter
☐ Developing a business case
☐ Chartering a six sigma team
☐ Defining roles and responsibilities
☐ Gathering voice of the customer and support for a project
☐ Translating customer needs into specific requirements
☐ Define phase review elements
Measure
☐ Process mapping (as-is process)
☐ Understanding data attributes (continuous versus discrete)
☐ Defining metrics
☐ Measurement system analysis
☐ Gauge repeatability and reproducibility
☐ Data collection techniques
☐ Calculating sample size
☐ Data collection plan
☐ Understanding variation
☐ Measuring process capability
☐ Calculating process sigma level
☐ Rolled throughput yield
☐ Visually displaying baseline performance
☐ Statistical software training
☐ Measurement phase review
Analyze
☐ Visually displaying data (histogram, run chart, Pareto chart, scatter diagram)
☐ Detailed (lower-level) process mapping of critical areas
☐ Value-added analysis
☐ Cause-and-effect analysis (fishbone, Ishikawa)
☐ Affinity diagram
☐ Data segmentation and stratification
☐ Correlation and regression (linear, multiple)

EXHIBIT 32.2 Black Belt Body of Knowledge

This exhibit contains references to some quality assurance terminology, such as fishbone and Ishikawa techniques, that are not included in this book. A Web search on the terms will provide more information.

- ☐ Process performance (Cp, CpK, Pp, PpK, CpM)
- ☐ Short-term versus long-term capability
- ☐ Nonnormal data distribution transformations
- ☐ Central limit theorem
- ☐ Goodness-of-fit testing
- ☐ Hypothesis testing
- ☐ Analysis of variance (ANOVA), two-sample T-Tests, Chi-squared test
- ☐ Design of experiments (DOE): full, fractional, factorials
- ☐ Verification of root causes
- ☐ Determining opportunity (defects and financial) for improvement
- ☐ Project charter review and revision
- ☐ Statistical software training
- ☐ Analyze phase review

Improve

- ☐ Brainstorming
- ☐ Multivoting
- ☐ Process simulation
- ☐ Quality function deployment (house of quality)
- ☐ Selecting a solution
- ☐ Failure modes and effects analysis (FMEA)
- ☐ Poka yoke (mistake-proofing your new process)
- ☐ Piloting your solution
- ☐ Implementation planning
- ☐ Statistical software training
- ☐ Culture modification planning for your organization
- ☐ Improve phase review

Control

- ☐ Assessing the results of process improvement
- ☐ Statistical process control (SPC)
- ☐ Rational subgroupings
- ☐ Establishing process standards for inputs, process, and outputs
- ☐ Developing a process control plan
- ☐ Documenting the process
- ☐ Statistical software training
- ☐ Control phase review

EXHIBIT 32.2 Black Belt Body of Knowledge (*Continued*)

Beyond these designated six sigma leaders, many others in an enterprise are usually assigned to a project to analyze and achieve results. The whole concept here is that a team of designated six sigma "belts" should study areas of operations to identify a process or service areas with objectives to eliminate errors or waste to bring operations down to the six sigma standard of less than 3.4 DPMO. This is a very tight standard. Internal auditors who are accustomed to reviewing documents for internal control violations but who sometimes give small violations a pass may find six sigma rules very strict. Six sigma has almost no tolerance for errors or exceptions. Even when an enterprise has not formally adopted an overall six sigma program, internal auditors should consider user using six sigma rules as part of their internal

audit activities. Section 32.5 discusses how to better introduce six sigma principles into an internal audit function.

(b) Launching the Six Sigma Project

A successful six sigma initiative in an enterprise does not require the implementation of one large project; many smaller efforts can initiate improvements. Like internal auditors performing reviews to improve internal controls, a six sigma team looks at virtually all processes and attempts to find opportunities for improvements. A critical difference is that internal auditors generally start with a high-level approach—such as a plan to review internal controls in some operating unit. The six sigma team typically develops detailed flowcharts covering both large and small operations and then asks these questions to better understand a process:

- For which stakeholder does a process primarily exist?
- What value does the process create or what outputs are produced?
- Who is the owner of the process?
- Who or what supporting area provides the inputs to the process?
- What are the inputs to the process?
- What resources—people, information technology (IT), or other—does this process use?
- Are there any subprocesses with their own discrete start and end points?
- What steps in the process create value?

Based on this preliminary information, the six sigma team then establishes some process improvement objectives. These can cover a wide variety of areas. Each process should be given a high-level objective, such as to "help customers better find the replacement parts needed for a product," to "improve product delivery times," or to "reduce office staff voice message telephone tag communications." The six sigma process can then look at all operations in the enterprise, ranging from major to the almost mundane.

The six sigma team then creates high-level process maps for each area reviewed, to the process maps described in Chapter 16. However, because six sigma improvements often emphasize activities outside of the enterprise, such as customers and suppliers, the analysis should cover their needs and requirements. Using six sigma terminology, a series of supplier-inputs-process-outputs-customer (SIPOC) charts should be created to describe the overall process. Exhibit 32.3 is an example SIPOC chart that describes customer service process in a personal car repair process.

The black belts who performed this SIPOC analysis should design and propose a six sigma process improvement project. Based on the data gathered, the team should document opportunities to improvement, estimate the potential cost savings, and then identify a sponsor from the business area reviewed. Usually a senior manager from some area of operations will recognize potential savings and will take responsibility for the expected process improvements. The proposed project is then be reviewed and approved as an active six sigma project. The overall management of any six sigma project is similar to the project management processes discussed in Chapter 14.

Six sigma projects follow the DMAIC steps discussed earlier. Exhibit 32.4 describes the use of these DMAIC procedures for a six sigma project. This should be

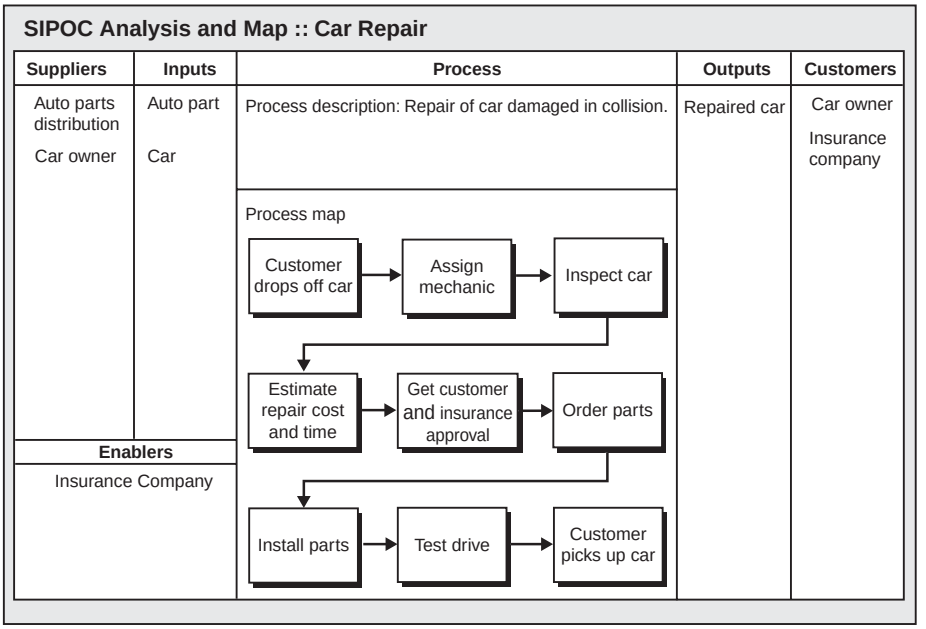


EXHIBIT 32.3 Six Sigma SIPOC Chart Example

Source: U.S. Army Business Transformations, www.armyBTKC/focus/cpi/tools3.

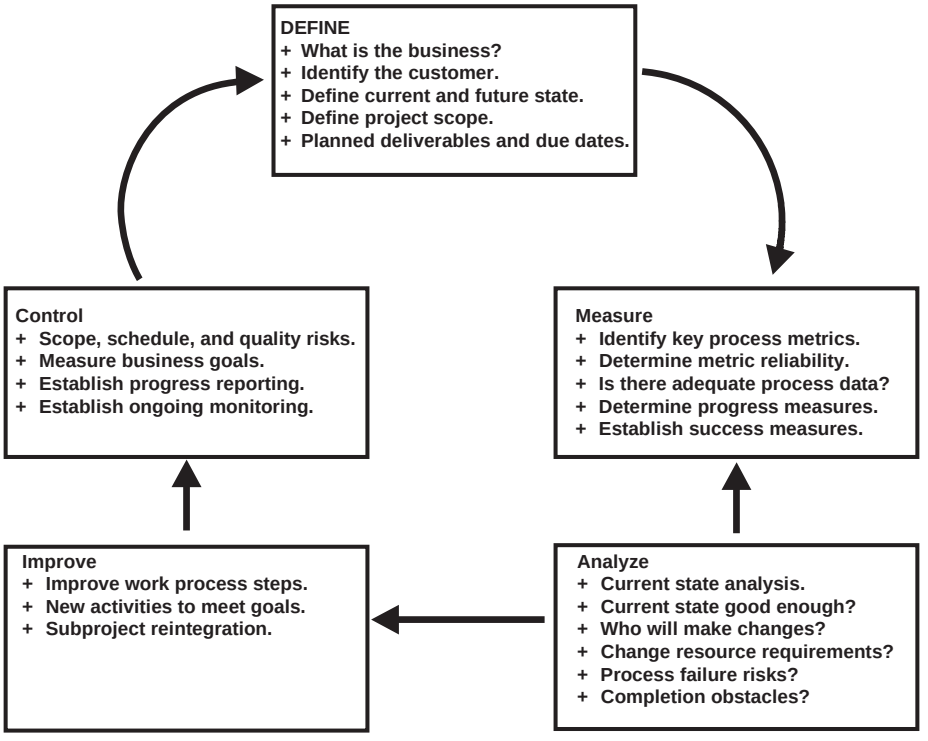


EXHIBIT 32.4 DMAIC Procedures for a Six Sigma Project

a repetitive process based on an objective of constant improvement. The first steps of defining the project are particularly important. Project goals, potential rates of investment returns, and such expectations as customer or employee satisfaction levels should be defined. The process of measuring, analyzing, and taking steps to improve the process follow. The final control steps call for the project team to implement and institutionalize the recommended and installed process improvements.

We have described six sigma here only at a very high level. To actually analyze and reengineer processes often requires very detailed mathematical and quantitative analysis procedures. Six sigma procedures, as discussed, really got started in the United States through Motorola's improved processes for first the manufacture of television sets and then handheld cellular telephones. Cell phones are small but very technical devices where quality is very important, and achieving six sigma quality is a challenge.

Internal auditors should work with their enterprise's quality and six sigma teams to learn more about how the concept is being applied. Often there are strong benefits for an internal auditor to work with or observe the black and green belt teams in their six sigma process improvement activities.

32.3 Lean Six Sigma

Around the same time that six sigma processes were launched in the United States, another initiative called lean manufacturing was launched. The efforts here came from U.S. auto manufacturers who were attempting to replicate techniques used by Japanese manufacturers such as Toyota. The main difference between these two concepts is that six sigma emphasizes quality while lean manufacturing emphasizes the speed of production. Over time, these concepts have somewhat merged together into what is called lean six sigma. This combined concept is based on the recognition by many industry leaders that you cannot do "just quality" or "just speed"; a balanced process is needed that can help an enterprise focus on improving service quality, as defined by the customer within a set time limit.

The service management concept of lean six sigma is increasingly being used by major enterprises. To cite one example, a recent *Fortune* magazine[1] contained an interview with Gary Reiner, chief information officer of General Electric. One of the questions was "What does Jeff Immelt [the CEO] want from you?" Reiner responded: "Three things. My responsibility for IT, Lean Six Sigma, and sourcing." The interview contains some other references to General Electric's use of lean six sigma.

The origins of lean manufacturing date back well into the late twentieth century (it was not called lean then). The word *lean* came from studies on the differences between some very successful Japanese carmakers and the traditional North American carmakers. The key thought processes within lean are the identifying of "waste" or "non–value-added activities" from the customer perspective and then determining how to eliminate them effectively. Waste is defined as the activities that a customer would not want to pay for and/or that adds no value to the product or service from the customer's perspective.

The determination of value is a key concept behind lean production or manufacturing. *Value* is an item or feature for which a customer is willing to pay. All other aspects of the process are deemed as waste. The lean framework has been used

as a tool to focus resources and energies on producing value-added features while identifying and eliminating non–value-added activities. Among other concepts, lean production emphasized improved quality assurance, manpower reductions, a focus on customer value, and the concept of just-in-time manufacturing. This latter concept says production materials do not need to be placed in stockrooms but should be introduced to the production process only when needed.

In the 1990s, lean and six sigma each had its own separate adherents, each arguing that one was better than the other. Eventually, specialists began to realize the lean techniques alone cannot bring a process under the statistical controls that are so important in reducing exceptions. However, six sigma alone cannot dramatically improve process speeds or reduce the need for invested capital. Thus lean six sigma was launched.

Lean six sigma uses many of the same tools and procedures that six sigma does. For example, a key component of any analysis here is the same basic DMAIC cycle approach shown in Exhibit 32.4. There is now much more emphasis on analyzing non–value-added components in a process and measuring process cycle efficiencies. The same black and green belts still identify and develop process improvement projects. The overall difference is not just on reducing statistical error rates to six sigma levels but establishing dramatic improvements in process efficiency and eliminating waste in all level of operations.

While efficiency improvements sometimes are hard to define with a strong set of statistical measures that form the backbone of six sigma, lean six sigma also emphasizes improvements in the overall process value stream and the elimination of waste. Exhibit 32.5 contains some examples of process waste. These are some of the areas that lean six sigma techniques attempt to reduce. Many internal auditors will recognize them as potential areas for improvement.

Internal auditors may wonder what the differences are between six sigma techniques and lean six sigma. In many respects, many people do not really understand

EXHIBIT 32.5 Lean Six Sigma Process Waste Example

Type of Waste	Process Improvement Waste Examples
Complexity	Unnecessary process or production steps, excessive or difficult-to-understand documentation, too many approval checkpoints
Labor	Excessive headcount, ineffective operations, poorly trained personnel
Overproduction	Producing more than customer demands or producing in advance of customer needs
Facility space	Storage for inventory excess, parts awaiting disposition, production material waiting rework or scrap storage; also, excessively wide aisles or other wasted, unused space
Energy resources	Wasted power requirements or demands for excessive human energy
Process defects	Repair, rework, multiple steps to resolve problems
Materials	Scrap, ordering more than is needed
Idle materials	Excess inventory, material that does not match requirements
Time	All human, machine, and IT processes that waste time
Transportation	Movements of any sort that add no value
Safety hazards	Unsafe or accident-prone environments

the fine differences between the two and refer to everything as six sigma. Pure six sigma is much more statistically process oriented; the lean approach emphasizes process improvements and the elimination of waste. This is often enough of a distinction for an internal auditor. The next sections discuss the auditing six sigma processes, but essentially they cover both regular and lean six sigma.

32.4 Auditing Six Sigma Processes

Internal auditors frequently encounter major six sigma initiatives at auditee locations. This has been particularly true for manufacturing-related operations but is becoming increasingly common in other areas of operations, such as financial service processing. Six sigma has been beyond the sphere of interest for most IIA-heritage internal auditors. For example, we mentioned earlier that the IIA Web site at the time of our publication contained no internal auditor references to six sigma. Also, because six sigma operations are often structured as a special project outside of normal organization charts, many times they do not appear or are not a consideration when building an audit universe and developing internal audit plans. This is a deficiency that many internal auditors need to correct.

A properly organized and structured six sigma project can bring some significant benefits to an enterprise, but it also can quickly become an expensive and even risky undertaking if not well managed and controlled. The benefits from a strong six sigma program are valuable, but problems can develop due to these issues:

- **Limited project management.** Six sigma requires well-thought-out projects with good objectives and detailed planning. These sometimes are missed when six sigma teams work on these projects along with their regular work duties.
- **Poor budget controls.** The excitement of launching a six sigma effort can create an almost open checkbook environment where no attention is given to costs—particularly in employee time costs—because it is *six sigma*. Projects sometimes lack strong project management controls.
- **Limited supporting documentation.** Concepts such as lean six sigma encourage professionals to trim down on the paperwork supporting six sigma results, and requirements here are very different from internal auditor supporting materials. Nevertheless, there always should be some level of documentation to corroborate six sigma results.
- **Failures to coordinate six sigma efforts.** Multiple six sigma teams may operate at almost cross-purposes among themselves and with normal enterprise operations. There is often a need for some multiproject program management.

These comments are not meant to criticize six sigma efforts but to highlight that in the enthusiasm to launch an initiative, matters sometimes get out of control. Internal audit can provide a strong service to overall management by scheduling an internal controls review of the overall enterprise six sigma effort or of individual larger projects.

A review of six sigma efforts often present internal audit with danger. Six sigma proponents will argue that the overall effort is designed to promote efficiency within the enterprise and any internal audit efforts may only hamper things. Internal audit

needs to point out its overall objective to review internal controls and its ability to assess the overall quality of such a program. Many six sigma efforts take place primarily on the factory floor while internal audit may be more oriented to corporate headquarters. Internal audit needs to bridge that gap.

A strong internal auditor understanding of the six sigma process is a key requirement. An internal auditor launching a review in this area, however, may very well encounter a comment along the lines of "I'm a black belt. What do you know about six sigma that qualifies you to audit me?" This, of course, is the same situation that an internal auditor will encounter in many other areas, whether launching a review of an IT function or a specialized financial area. Through reading, general studies, and discussions with quality auditors, internal audit should exhibit enough knowledge of six sigma processes to have a general understanding of this area. However, any internal audit should be based on a good general assessment of the internal controls environment in the area, whether six sigma or any other,

Exhibit 32.6 lists some internal audit procedures for a review of an enterprise six sigma program. While any review would cover specific six sigma projects, the review might best be focused on the overall program, with an emphasis on project management processes, as discussed in Chapter 14, as well as general budget and financial controls covering the project. Depending on the nature and scope of the overall six sigma program, internal audit may want to either observe or participate in one or more selected projects. Properly executed, an internal audit review of an enterprise six sigma project should help to strengthen and increase the importance of the overall project.

32.5 Six Sigma in Internal Audit Operations

Six sigma is a process to increase customer satisfaction by dramatically reducing the number of process exceptions. It has its origins in high-production-level manufacturing operations, such as cell phone handsets. Lean six sigma is more process oriented and has found use in high-volume financial services operations. However, there is no reason why some of these six sigma concepts cannot be directly implemented in internal audit operations. As discussed in Chapter 8, there is a strong requirement for internal audit to establish effective quality assurance standards. Effective quality assurance can be enhanced by establishing six sigma (e.g., programs to better monitor performance, reduce exceptions, and improve the overall quality of internal audit operations).

Because almost every scheduled internal audit will be different, many of the six sigma principles discussed in this chapter will not apply to regular internal audit operations. However, the basic six sigma concepts of closely monitoring activities and eliminating errors and exceptions are very important. For example, on both an internal audit department and individual level, a strong emphasis should be placed on accurately planning internal audit start and completion dates, including the issuance of audit reports. Meeting or bettering those dates should receive major emphasis. Similarly, a strong no-errors emphasis should be placed on the accuracy of all audit findings and reported results. These actions will improve the overall quality of internal audit activities and will help others in the enterprise realize that internal audit is following six sigma principles.

EXHIBIT 32.6 Internal Audit Procedures for a Review of a Six Sigma Program

1. Plan and schedule the audit.
   - 1.1. Establish high-level objectives for the review.
   - 1.2. Confirm planned review with audit committee, senior management, and persons responsible for six sigma activities.
   - 1.3. Arrange for six sigma training for audit staff members performing review.
   - 1.4. Schedule audit per normal internal audit planning cycle.
2. Review and understand six sigma organization.
   - 2.1. Understand six sigma organization and meet with director to understand recent achievements and current projects.
   - 2.2. Understand number and responsibilities of master, black, and green belts assigned to six sigma projects.
     - 2.2.1. Determine that adequate procedures are in place for belt certifications.
     - 2.2.2. Review adequacy of six sigma team operating procedures for such areas as documentation of reviews, testing procedures, and documentation requirements.
   - 2.3. Review and assess adequacy of six sigma budgeting processes in place, and assess reasons for any significant variances.
   - 2.4. Review overall effectiveness of the six sigma deployment, including supporting systems, communications processes, and recognition systems.
3. Review and assess six sigma project management processes.
   - 3.1. Review procedures for developing, planning, and managing six sigma projects to determine that they are consistent with good project management procedures (see Chapter 14).
   - 3.2. Determine that appropriate objectives, such as cost-per-unit measures, have been established and are monitored in six sigma projects.
   - 3.3. On a sample basis, review project documentation for completed six sigma projects to determine adequacy and completeness of processes.
   - 3.4. Determine that adequate procedures are in place for reporting progress and results of six sigma projects to overall enterprise.
4. Select one or more completed six sigma projects and assess whether adequate attention was given to DMAIC steps for each selected project.
   - 4.1. Define steps. Objectives of each project should be clearly defined along with an analysis of current state, planned future state, due dates, and deliverables.
   - 4.2. Measure steps. Key metrics should be established along with processes to use those metrics to achieve project success.
   - 4.3. Analyze steps. Evidence should be in place to determine that current state benchmarks were established as well as measurement results that will point to measurable process improvements.
   - 4.4. Improvement steps. Processes should be in place, including measurement tools, to implement suggested improvements or approaches.
   - 4.5. Control steps for new processes. Measurement steps should be in place to demonstrate new process is working as predicted or, if not, to revise for next round of improvements.
5. Assess adequacy and completeness of six sigma deployment.
   - 5.1. Where appropriate, review adequacy of selected completed six sigma projects for their emphasis on:
     - 5.1.1. Asset utilization improvements.
     - 5.1.2. Profit and revenue improvements.
     - 5.1.3. Service and customer relationship improvements.
     - 5.1.4. Product introduction and process improvements.
   - 5.2. Determine that adequate processes are in place to analyze results and initiate corrective actions.
   - 5.3. On a sample basis, select several six sigma projects that have been implemented recently and assess if objectives have been met adequately.
6. Determine that adequate communication tools are in place to report results of six sigma work to all constituents.

Six sigma, and in particular lean six sigma, has been a major initiative at many enterprises worldwide for some years. With many demonstrated success stories surrounding it, we can expect to see more implementations to improve customer service and massively reduce errors and exceptions. While they probably will not have black or green belt levels of knowledge, internal auditors should develop a broad general CBOK understanding of six sigma principles. In this way, they can demonstrate a knowledge and understanding of this important concept in much of their internal audit activities.

Note

1. "Information Worth Billions . . ." *Fortune,* July 21, 2008, p. 73.

CHAPTER 33

International Internal Auditing and Accounting Standards

As internal commerce and communications becomes more and more global, there is a strong need for business and commercial standards to converge. The Internet would not be very effective, for example, if each country had its own transmission and transfer protocol such that a Web message sent from Chicago to someone in Canada could not go beyond the national boundary or at least had to go through some kind of cross-border conversion. There are many reasons to have national standards, but business and commercial considerations point to the advantage of common standards.

This chapter briefly looks at two areas of internal audit interest where standards are becoming more common. The first is the "make the debits equal the credits" international accounting and financial reporting standards. In past years, different accounting standards existed in many countries. For example, there were many small but nagging accounting and financial reporting standard differences among France, Germany, and Belgium. Over the years, first with the European Union and then through much of the rest of the world, international financial reporting standards (IFRS) were developed and came to be generally accepted. The one major holdout through 2008 was the United States. The rules have now changed, and as of late 2008, the U.S. Securities and Exchange Commission (SEC) has mandated a conversion to IFRS as well.

While internal auditors typically are not directly involved with financial reporting and accounting issues, this conversion to IFRS will have some internal audit implications for enterprises in the United States and elsewhere. This chapter briefly looks at IFRS and some of the internal controls conversion milestones that may have internal audit impacts.

This chapter also discusses internal auditing standards from a worldwide perspective. Although the Institute of Internal Auditors (IIA) professional practice standards, as discussed in Chapter 8, are receiving worldwide acceptance, there are other auditing standards of which internal auditors need at least to be aware. Internal auditors need a common body of knowledge (CBOK) general awareness but not necessarily a strong and detailed knowledge of the worldwide status of internal auditing standards and IFRS.

33.1 International Accounting and Auditing Standards: How Did We Get Here?

For many years, U.S.-based internal and external auditors had thought of the American Institute of Certified Public Accountants (AICPA) and its Auditing Standards Board (ASB) as the one body that established auditing standards for U.S. organizations. At least, that was prior to the Sarbanes-Oxley Act (SOx) and the Public Corporation Auditing Oversight Board (PCAOB), discussed in Chapter 4, which now has the authority to establish U.S. auditing standards. Of course, the whole purpose of any audit is to review compliance against some recognized standard or principle. One of the major tenets of internal control, under the Committee of Sponsoring Organizations and any other internal audit, is compliance with laws and regulations. That legal compliance becomes a standard for audits of internal accounting controls. Financial audits also assess the fairness of accounting procedures per established accounting standards. Those standards in the United States have been based on the long-standing concept of generally accepted accounting principles (GAAP) as well as very specific accounting rules prescribed by the Financial Accounting Standards Board (FASB), an independent rule-setting accounting standards authority. The U.S. auditing and accounting standards, however, are not certainly used throughout the world.

Standards such as double-entry bookkeeping are accepted and recognized throughout the world. Others may have the same intent but may be different in various national entities. The practice of driving on the right- or left-hand side of the road is such an example of a national practice. No matter which standard is followed, automobile drivers still can get from point A to B as long as all drivers follow the same correct-side-of-the-road rule. The same is true for auditing and accounting standards and practices. It becomes a bit more complex because we are an increasingly global economy, and accounting and auditing practices in Belgium, for example, need to be comparable to those of nearby France as well as Canada. In addition, there is a need for some consistency between Germany or the United States and both of those countries. As our individual organizations become increasingly global, internal auditors should at least have a general understanding of the differences and consistencies across international borders.

Accounting and auditing standards were established over the years on a country-by-country basis by professional or governmental boards as well as by some international standards-setting bodies. Individual countries may fully or only generally accept these international standards (the United States is an example of the latter). With strong established practices in many areas, the United States often takes the lead for establishing some of these international standards but goes its own way regarding other standards. That is, the United States accepts some international rules but ignores others. An example might be inch and foot versus meter measurement systems. The United States follows its own traditional system, but almost all of the rest of the world follows another. All internal auditors, no matter where they are located, should gain a general understanding of these rules and how they might apply to their organization and the national body that establishes the standards.

We are becoming a global economy. As we move into the world of international organizations, we run into a gaggle of initials to describe the regulatory agencies. The United Nations (UN) is a prime example, with its UNESCO, FAO, UNICEF, UNCTAD, and many more. International auditing and accounting standards often use similar sets of initials, which adds to the confusion. There are International Standards

of Auditing (ISAs) as well as International Accounting Standards (IASs). The ISA auditing standards are established by the International Federation of Accountants (IFAC) through its International Auditing and Assurance Standards Board (IAASB) which issues these ISAs as well as International Auditing Practice Statements (IAPSs). To complicate the picture, there is also the International Organization of Supreme Audit Institutions (INTOSAI) whose Auditing Standards Committee contributes to the work of IAASB.

Now the International Accounting Standards Board (IASB) sets the international financial reporting rules, called the international financial reporting standards (IFRS). The IASB is an independent accounting standard-setting body, based in London. It began operations in 2001, when it succeeded the International Accounting Standards Committee, and it consists of 14 members from 9 countries, including the United States. The ISAB is responsible for developing IFRS rules.

The IASB auditing standards are fairly consistent with the U.S. pre-SOx auditing standards that were issued by the ASB. Exhibit 33.1 lists the current IASB international auditing standards and IFRS international financial reporting standards. Even in their topics, these international standards are not totally consistent with the U.S. financial reporting and auditing standards documents. The international standards are general principles; U.S. standards tend to be very specific rules. The IFRS and IASBs are released after publication of an exposure draft and are published in over 20 languages. More than 100 countries have indicated that they either have adopted these international standards or feel there are no significant differences between their own national standards and the IFRS standards. The United States has been one of the "no significant differences" countries here. In many cases and until the PCAOB assumed responsibility for U.S. auditing standards, the IASB's standards followed the issuance of U.S. Statement on Auditing Standards (SAS) documents. For example, IASB 240 on fraud closely follows SAS No. 99 on auditing for fraud, as discussed in Chapter 25. Today's typical internal auditor does not need to have a detailed understanding of these international standards of auditing. However, as we work in a more global environment, they will become increasingly important.

The International Accounting Standards Board (IASB) publishes accounting standards in a series of pronouncements called International Financial Reporting Standards (IFRS), as shown on Exhibit 33.1. Those pronouncements continue to be designated International Financial Reporting Standards" (IFRS) and International Auditing Standards (IAS). They provide somewhat of a basis for all counties worldwide and, in particular, provide accounting standards for a developing country that does not have established standards. Most developed countries have established accounting standards that generally follow U.S., British, German, Swiss, or French standards. The IAS standards historically were not inconsistent with those country-by-country standards. An internal auditor doing work in a developing country that does not have any strong accounting standards should look to the IAS materials to form a basis for appropriate accounting standards.

33.2 Financial Reporting Standards Convergence

With our international economy, there has been a growing need to report financial results using the same rules worldwide. A company headquartered in the United States but with large operations in Germany historically has had to report its financial

EXHIBIT 33.1 International Financial Reporting and Auditing Standards as of January 2008

International Financial Reporting Standards (IFRSs)

- **IFRS 1** First-Time Adoption of International Financial Reporting Standards
- **IFRS 2** Share-Based Payment
- **IFRS 3** Business Combinations
- **IFRS 4** Insurance Contracts
- **IFRS 5** Non-Current Assets Held for Sale and Discontinued Operations
- **IFRS 6** Exploration for and evaluation of Mineral Resources
- **IFRS 7** Financial Instruments: Disclosures
- **IFRS 8** Operating Segments

International Accounting Standards (IASs)

- **IAS 1** Presentation of Financial Statements
- **IAS 2** Inventories
- **IAS 7** Cash Flow Statements
- **IAS 8** Accounting Policies, Changes in Accounting Estimates and Errors
- **IAS 10** Events After the Balance Sheet Date
- **IAS 11** Construction Contracts
- **IAS 12** Income Taxes
- **IAS 16** Property, Plant and Equipment
- **IAS 17** Leases
- **IAS 18** Revenue
- **IAS 19** Employee Benefits
- **IAS 20** Accounting for Government Grants and Disclosure of Government Assistance
- **IAS 21** The Effects of Changes in Foreign Exchange Rates
- **IAS 23** Borrowing Costs
- **IAS 24** Related Party Disclosures
- **IAS 26** Accounting and Reporting by Retirement Benefit Plans
- **IAS 27** Consolidated and Separate Financial Statements
- **IAS 28** Investments in Associates
- **IAS 29** Financial Reporting in Hyperinflationary Economies
- **IAS 31** Interests in Joint Ventures
- **IAS 32** Financial Instruments: Presentation
- **IAS 33** Earnings per Share
- **IAS 34** Interim Financial Reporting
- **IAS 36** Impairment of Assets
- **IAS 37** Provisions, Contingent Liabilities and Contingent Assets
- **IAS 38** Intangible Assets
- **IAS 39** Financial Instruments: Recognition and Measurement
- **IAS 40** Investment Property
- **IAS 41** Agriculture

Source: International Accounting Standards Board, www.iasb.org

results using both U.S. and once German and now European Union rules. In a step toward eliminating the existing differences between U.S. GAAP and international standards, FASB and IASB examined and selected the better of these standards in each of 15 areas, including how companies make restatements when accounting standards change and in the classification of short- and long-term liabilities. This effort toward harmonization came when all publicly-listed European companies as well as many located elsewhere have met international accounting standards. The United States had been the exception here.

The increasing integration of the world's capital markets, which has resulted in two-thirds of U.S. investors owning securities issued by foreign companies that report their financial information using IFRS, also has made the establishment of a single set of high-quality accounting standards a matter of growing importance. A common accounting language around the world could give investors greater comparability and greater confidence in the transparency of financial reporting worldwide.

Although there has been a frequently discussed goal to reach a consensus on standards, with a series of "road maps" whose dates were never met, the SEC finally took some definitive action. In August 2008, the SEC voted to publish for public comment a proposed road map that could lead to the use of IFRS by U.S. issuers beginning in 2014. The SEC has stated it would make a decision in 2011 on whether adoption of IFRS is in the public interest and would benefit investors. The proposed multiyear plan sets out several milestones that, if achieved, could lead to the use of IFRS by U.S. issuers in their filings with the SEC.

While we have no way to predict what will happen regarding the U.S. transition from GAAP to IFRS, many influential players, such as the AICPA, are in favor of this move, and many predict that the U.S. conversion should start the transition sometime between 2011 and 2014. Any GAAP to IFRS conversion will probably occur in a staged manner, with large corporations first, similar to the way corporations were required to convert to SOx.

The conversion from GAAP to IFRS will not be a simple slam-dunk. There are many subtle differences that will impact financial reporting, employee benefit plans, management reporting, and much more. As just a single example, many U.S. corporations use what is called last-in-first-out (LIFO) accounting rules in accounting for their inventories. The idea is that although an enterprise may buy an inventory item at various times and often rising prices, when it sells an inventory item, it will take it out at the cost of the most recent higher-priced item. A concept that was very useful during periods of higher inflation and before the just-in-time smaller stock inventories used today, LIFO inventory accounting is very common in the United States. IFRS does not allow LIFO. This means that as a U.S. enterprise converts to IFRS, it will face some substantial inventory accounting and information technology (IT) systems problems.

What does this type of change mean to a U.S.-based corporation? Beyond a change to its financial accounting processes, the IT systems for inventory control and job cost accounting will almost certainly be impacted. This will also be an area for potential internal audit help.

33.3 IFRS: What Internal Auditors Need to Know

The increasing acceptance of IFRS, both in the United States and worldwide, means that internal auditors should become knowledgeable about IFRS and the differences between it and U.S. standards. Many U.S.-based internal auditors may be affected. Once a critical mass in various industries begins to report their financial results using IFRS, even if before an SEC-imposed deadline, there will likely be pressure for noncompliant issuers to do the same to allow investors to better compare their financial results. Such a conversion to IFRS will have an impact beyond the last financial reports. It may affect almost every aspect of a U.S. company's operation,

including its IT systems, its tax reporting requirements, and even the way it tracks stock-based compensation.

For internal auditors, the use of IFRS by U.S. public corporations will create a need for effective training and education among the financial staff. Enterprises will use IFRS only if they and their external and internal auditors have been thoroughly trained and if users of their financial statements—such as analysts and rating agencies—understand it. Most U.S.-based internal auditors who perform primarily financial internal controls audits are trained in U.S. GAAP, not IFRS. In order to have a better understanding of IFRS, internal auditors need to learn about it through reading and training. As IFRS becomes accepted in the United States, internal auditors need to embark on a comprehensive training program to learn more about these international standards.

For U.S.-based internal auditors, IFRS is almost certainly coming. At the time of this publication, the IIA Web site (theiia.org) offers no help; nor does the Information Systems Audit and Control Association (ISACA) provide any guidance. More study materials will become available, but to learn more about IFRS today, the AICPA Web site (www.aicpa.org) can be of help, and a search on Google will point to other sources.

As a point of clarification, IFRS will officially impact only SEC-registered public corporations. It does not apply to a wide variety of nonpublic entities, such as partnerships, nonprofits, and governmental entities. However, once it becomes widespread for U.S. public corporations, we can expect to see a universal implementation.

33.4 International Internal Auditing Standards

The IIA's *International Standards for the Professional Practice of Internal Auditing,* as summarized in Chapter 8, have become the worldwide standard for internal auditing. A search on Google returns references pointing mainly to these IIA standards. However, the ISO-based international auditing standards, highlighted in Chapter 30, may have an increasingly important impact in future years.

ISO 100011 is a quality auditing international standard. There are three sections to this standard (cited with the year it was issued):

ISO 10011–1: 1990—Quality Audit Objectives
ISO 10011–2: 1990—Quality Audit Educational Objective
ISO 10011–3: 1990—Develop the Quality Audit Management Process

Detailed descriptions of these standards that are available through the ISO Web site (www.iso.org). Each standard consists of detailed subsections. For example, ISO 10011–3 contains sections on (1) developing the audit management process, (2) selecting the audit manager, (3) selecting auditors, (4) selecting lead auditors, (5) managing the process, (6) supporting the process, and (7) supporting continuous improvement. Each standard is supported by very detailed sets of standards materials to support these quality audit processes. To give a flavor of these standards, Exhibit 33.2 contains a summary of the standard to manage the audit process. The exhibit contains high-level summary descriptions; the actual published ISO standard contains very precise, detailed directions.

EXHIBIT 33.2 ISO 10011–3 on Managing the Audit Process

An audit manager should manage the audit process. The audit manager should:

- Ensure that all auditors and lead auditors are knowledgeable and suitably trained.
- Develop and enforce a code of ethics to govern the audit process.
- Monitor and evaluate the performance of their audit team in order to improve their efficiency and effectiveness.
- Ensure that all auditors make the same observations and draw the same conclusions when confronted with the same evidence. Audit managers should help guarantee consistency.

The ISO 9000 standard talks about the need for a quality audit process to review each standard. ISO 10011 defines the audit standards to audit other ISO standards. ISO standards and quality auditing represent a very different direction from that of today's IIA-heritage internal auditor. However, a general knowledge and understanding of these standards will be important and should be a CBOK general understanding for all internal auditors.

33.5 Next Steps in Internal Audit Standards

We do not anticipate any major standards changes impacting internal auditors in the near future. However, the probable change to IFRS in the United States will have a major impact on U.S.-based internal auditors in many enterprises. Conversion is still uncertain, but if the United States wishes to remain a major global competitor, the IFRS adoption is almost certain.

The IIA's standards, as discussed in Chapter 8, will almost certainly continue as the worldwide internal audit standard. However, ISO standards such as 100011 will increase in their importance, perhaps almost to the point where there may be a greater level of convergence. Every internal auditor should have a high-level CBOK awareness and understanding of appropriate ISO standards, such as 100011, and should apply them in regular internal audit processes when appropriate.

CHAPTER 34

CBOK for the Modern Internal Auditor

Chapters 1 and 2 introduced the need for an internal auditor common body of knowledge (CBOK), a body or set of knowledge areas where all internal auditors should have either a strong or a good understanding. We also discussed the efforts of the Internal Auditors Association Research Foundation (IIARF) to outline a current status internal audit CBOK based not on what internal auditors should know but through internal auditor surveys over past years. These IIARF survey results told what internal auditors were doing as of 2006 but also reported some troubling results.

While we did not have access to all of the data, the IIARF CBOK survey found that some internal auditors were not even following their own professional standards. For example, Table 5–8 in the IIARF's final CBOK study[1] reports that only some 90% of the chief audit executives (CAEs) surveyed felt that their internal audit function "adds value" and "proactively examines important financial matters, risks, and internal controls" in the CAE's enterprises. These are areas where we would have expected that nearly 100% of CAEs should be in agreement. These and other similar troubling reported statistics led to our objective to not rely on a survey to define internal audit practices but to better define an internal audit CBOK.

Our internal auditor CBOK, as discussed throughout this book, is not based on multiple surveys but on this author's 30+ years of experience in many aspects of internal auditing as well as published standards. We have tried to define our CBOK in terms of some key areas where all internal auditors must have a strong level or knowledge and understanding—such as adherence to internal audit standards—as well as other areas where we recommend that internal auditors should have at least a good general knowledge.

Our description of an internal auditor CBOK is much greater than just a series of bullet points to be summarized on a single chart. The framework for our internal auditor CBOK has been discussed in previous chapters. Here we define an internal auditor CBOK by revisiting each of the eight parts of this book with a summary of CBOK needs described in the supporting chapters. Of course, any of these knowledge areas could be expanded in much greater detail. For example, Chapter 9 provided an overview of audit sampling and suggested that all internal auditors should have a CBOK understanding of sampling techniques. That chapter only highlighted key areas where internal auditors should understand audit sampling; an internal auditor may need to dig a bit deeper, through other references and technical seminars, to build that CBOK level of knowledge.

34.1 Part One: Foundations of Modern Internal Auditing

Chapters 1 and 2 discussed the background and origins of the profession of internal auditing and introduced the need for an internal audit CBOK. A CBOK is a basic concept discussed throughout this book, and we have provided some well-recognized definitions of the internal auditing profession. Professionals at all levels of their careers frequently are asked: "What does an internal auditor do?" Chapter 1 provided some basic internal auditor definitions—an essential CBOK requirement.

Chapter 2 provided some background on the origins and need for an internal audit CBOK. Due to the various industries and geographical areas where internal auditors operate in evaluating internal controls and assisting management, there can be many variations in their modes and styles of operations. However, all internal auditors should have some basic skills and competencies—a CBOK. All internal auditors should understand why a CBOK is important for their profession and why they should always try to follow CBOK best practices in every aspect of their internal audit work.

34.2 Part Two: Importance of Internal Controls

The four chapters in this section introduced some common practices that are essential knowledge requirements for every internal auditor. Chapter 3 discussed how many enterprises and their internal auditors went for years without a clear and consistent understanding of the meaning and concept of internal controls. Definitions were resolved and clarified, however, through the Committee of Sponsoring Organizations (COSO) internal controls framework, a three-dimensional description or framework of how an enterprise should organize and think of its internal controls. Originally launched as sort of best practice description of what constitutes good internal controls, the COSO internal controls framework has become a standard for defining and establishing good internal controls, first in the United States and now worldwide. Whether in an industry environment, as an information technology (IT) specialist internal auditor, or in not-for-profit or governmental sectors, every internal auditor should possess a CBOK understanding of the COSO internal controls framework.

In the early part of the twenty-first century, a series of major accounting frauds and business failures became a clarion call for external auditing and corporate governance reforms. The result was the Sarbanes-Oxley Act (SOx) in the United States, as discussed in Chapter 4. While SOx's initial focus was on larger U.S. corporations, it has defined rules and reporting standards that are requirements for many enterprises—large and small—in the United States and worldwide. The overall SOx legislation is very broad and has some regulations and rules that may be of little interest to most internal auditors, but a knowledge and understanding of the SOx internal control review procedures should be a CBOK requirement for all internal auditors who work with public corporations. In addition, all internal auditors should have general CBOK understanding of the SOx internal control and its corporate governance rules.

Chapter 5 introduced another very important internal controls framework, *C*ontrol *ob*jectives for *i*nformation and related *T*echnology (CobiT). An internal controls framework with origins tied to IT audit specialists, CobiT is important for all

internal auditors because IT systems and processes are so pervasive in all aspects of every enterprise. Whether operational, financial, or IT specialists, all internal auditors should have at least a high-level CBOK understanding of the CobiT framework and how it might apply to their internal audit activities.

Chapter 6 presented the COSO enterprise risk management (COSO ERM) framework, a model to help understand and describe enterprise risk management. A basic understanding of the concepts and principles of risk management is important for all internal auditors today, to help them assess areas to review and make other internal audit decisions. Every internal auditor also should have a high-level CBOK understanding of COSO ERM.

34.3 Part Three: Planning and Performing Internal Audits

Having a good knowledge and understanding of such areas as COSO internal controls will help an internal auditor to understand some basic principles, but an internal auditor needs to know how to plan and perform internal audits. The five chapters in Part Three included some of this CBOK background information, starting with Chapter 7 on performing effective internal audits. That chapter emphasized that the ability to plan and perform an individual internal audit is a key CBOK requirement.

A very strong knowledge and understanding of the Institute of Internal Auditors' (IIA's) *International Standards for the Professional Practice of Internal Auditing* is a key internal audit CBOK requirement. These standards are the rules outlining how an internal auditor should launch, conduct, and manage any review, whether an audit attest engagement or serving as an internal consultant. These are internal audit's marching orders.

While their technical details can be a challenge, all internal auditors should have a CBOK high level of understanding of statistical and nonstatistical audit sampling techniques. Audit sampling is a key knowledge area. Internal auditors should know how to look at a body of audit evidence, pull and review an appropriate sample of items from that evidence, and then make an audit decision and recommendations from that sample.

Internal auditors should perform their reviews using what are called audit programs, documented steps covering the audit procedures to follow. Internal auditors, at all levels, should understand how to construct and use audit programs, which serve as a guide for constructing consistent internal audit reviews. Chapter 11 covered another important area where internal auditors should have the knowledge and ability to perform self-audits and to assess how peer groups are performing similar internal audit functions. Called controls self-assessments and benchmarking, these are internal audit CBOK knowledge areas. Although not a knowledge requirement, internal auditors should have a general knowledge of these self-assessment processes.

34.4 Part Four: Organizing and Managing Internal Audit Activities

The six chapters in Part Four covered important CBOK areas on how an internal audit function should manage and perform audits as well as some individual internal audit skills. For example, Chapter 12 discussed audit charters, the official enterprise

audit committee authorizations of an internal audit function. Chapter 13 discussed some key internal audit competencies, the kinds of attributes that internal auditors should have in order to effective. Both of these cover CBOK areas that are essential for effective internal auditing.

Chapters 14 and 15 covered individual auditor and audit function activities. For example, understanding project management is discussed in Chapter 14. Virtually every internal audit project should be planned and organized in a well-structured, consistent manner, and the chapter provides an overview of understanding project management—a CBOK general knowledge requirement. Focusing on the individual internal auditor, Chapter 15 discussed the CBOK general steps necessary to plan and perform an individual internal audit, using a hypothetical example.

Chapter 16 covered an essential internal auditor CBOK area: documenting audit results through workpapers. Although detailed process and techniques may vary from one internal audit function to another, all internal auditors should have the knowledge and understanding of how to develop effective workpapers to describe individual audit activities. Ending this section, Chapter 17 discussed building effective internal audit reports, an essential internal audit method of communication. The ability to report internal audit results through effective audit reports is a key CBOK requirement. Although much of the effort is developing and delivering formal internal audit reports often is delegated to more senior members in the internal audit team, all internal auditors should have a strong CBOK understanding of the purposes and roles of their enterprise's internal audit reports.

34.5 Part Five: Impact of Information Technology on Internal Auditing

Because IT processes are so critical to all areas of business and other operations today, the five chapters of Part Five described some very important CBOK areas. Chapter 18 discussed performing IT general controls as well the Information Technology Infrastructure Library (ITIL) best practices for understanding and installing IT infrastructure controls procedures. These are CBOK areas where every internal auditor should have a general understanding.

The general controls that cover the overall IT function are important, but internal controls covering specific IT applications are at least as important. A CBOK understanding of these IT control concepts is particularly important for virtually all internal auditors, as many IT applications and their internal control responsibilities have moved from traditional centralized IT functions to individual user-managed controls. Internal auditors should have a good CBOK understanding of IT application controls, as discussed in Chapter 19.

With our heavy reliance on IT applications and processes as well as the use of the Internet and networked applications and IT resources, these same applications face a multitude of security and privacy threats. Chapter 20 discussed cybersecurity and IT privacy controls. While IT security issues are often a very special and complex area, internal auditors should try to gain an overall, high-level CBOK understanding of cybersecurity internal control issues.

Just as internal auditors need to understand key internal control principles, they also should be able to use that understanding to let IT processes aid them in their internal audit procedures. Chapter 21 discussed computer-assisted auditing tools and techniques (CAATTs), the processes to use IT tools to make other internal audits

more efficient. There are many potential approaches and techniques here. Internal auditors should have a CBOK general understanding of CAATTs and what can be done to make internal audits more efficient and productive.

Chapter 22 discussed business continuity planning and disaster recovery. This is an area where in recent years technology has made it much easier than in past years for an enterprise to save its IT-stored data to recover operations in the event of some unexpected event. One of the areas that was once very much the realm of IT specialist auditors, every internal auditor today should have a CBOK general understanding of continuity planning and recovery operations today.

34.6 Part Six: Internal Audit and Enterprise Governance

Events such as the enactment of SOx, a growing recognition of the importance of enterprise-level fraud, and other new laws have made many aspects of the business world increasingly complex and have added to an internal auditor's CBOK needs. The four chapters in Part Six looked at several areas where internal auditors should develop a CBOK general understanding.

Chapter 23 discussed internal audit communications and relationships with the board of director's audit committee. This is a critical requirement for the CAE, but all members of an internal audit function should have a general CBOK understanding of the role of an audit committee in internal audit operations and, in particular, that role in their own enterprise. Chapter 24 discussed ethics and whistleblower programs, important initiatives in many enterprises. Again, these are areas where internal auditors need to develop a good CBOK understanding of effective programs and why they are important to internal audit.

Understanding basic fraud detection and prevention controls, as discussed in Chapter 25, should be a CBOK requirement for all internal auditors. All internal auditors should gain a good CBOK level of understanding of both the red flags that indicate a possibility of fraud and general internal audit fraud investigation review procedures.

Chapter 26 discussed several more recent U.S.-based laws—the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA)—that have some strong enterprise-level compliance requirements. U.S.-based internal auditors should gain a CBOK general understanding of these and related compliance regulations; internal auditors elsewhere should develop similar CBOK understandings of the rules that govern compliance in their own locations.

34.7 Part Seven: The Professional Internal Auditor

Part Seven looked at several important CBOK areas. Chapter 27 discussed internal audit professional certifications, with an emphasis on the Certified Internal Auditor (CIA) and the Certified Information Systems Auditor (CISA) designations. While attainment of either of these designations is not necessarily a CBOK requirement, all internal auditors should have an understanding of these professional certifications and the requirements to achieve them. Internal auditors should strive to attain one or both of these credentials.

Chapter 28 discussed the role of the internal auditor as a business consultant. Internal audit standards banned that practice until recently, but today serving as an internal consultant can be a very important role for internal audit and its enterprise organization. Internal auditors should have a good general CBOK understanding of the internal audit rules for serving as an enterprise consultant.

This part concluded with Chapter 29 on continuous assurance auditing and a protocol called XBRL, where either internal audit or user management can improve financial reporting and install self-auditing procedures as part of normal business reporting. These areas have been proposed and discussed over the years with few successful implementations. Now they may be becoming more common, and internal auditors should gain a high-level CBOK understanding of each technique.

34.8 Part Eight: Internal Auditing Professional Convergence CBOK Requirements

The last part of our CBOK requirements discussion introduced the need for internal auditors to have a greater understanding of some issues that go beyond IIA-related internal auditing and its standards. For example, Chapter 30 introduced the international standards of the International Standards Organization (ISO). These standards and the compliance efforts to meet them have been in place worldwide for some years. They are increasingly appearing in U.S. environments, and internal auditors who work in IIA-standards environment should gain a greater CBOK understanding of them and their supporting concepts.

Chapters 31 and 32 introduced the whole area of quality internal auditing and quality processes. In the United States, these procedures are controlled by the American Society for Quality (ASQ) and have much in common with the IIA processes discussed throughout most of these chapters. Although the IIA and the ASQ operate almost separately today, there will almost certainly be a convergence of some IIA and ASQ procedures going forward. All internal auditors should develop at least a CBOK understanding of the ASQ quality internal audit standards and procedures.

Our discussion of quality processes in Chapter 32 included an introduction to an improvement process called six sigma, a methodology for enterprises to reduce errors and improve process efficiencies. Internal auditors should have a general CBOK understanding of six sigma and how it may be used in their enterprises.

Chapter 33 very briefly introduced some worldwide accounting and auditing standards. International accounting standards have been the preferred standards almost everywhere in the world except for the United States, which uses generally accepted accounting principles (GAAP). The United States is now taking steps to move from GAAP to the international standards. While this does not have a major impact on internal audit procedures, all internal auditors should have a CBOK understanding of a few of the implications of this change.

34.9 A CBOK for Internal Auditors

The topics summarized in this chapter and presented in more detail throughout this book outline a CBOK for internal auditors today. This CBOK covers many areas that may be beyond an internal auditor's immediate needs and requirements. However,

all internal auditors—from the CAE responsible for a large enterprise internal audit function to the student considering internal auditing as a career choice—should understand this large body of knowledge that represents the world of internal auditing.

This edition has attempted to paint a big picture of internal auditing in our ever-changing world. While many of the internal audit CBOK requirements described throughout these chapters will continue to be important and significant, other areas of emphasis may change in the years going forward. A future new edition here may point a slightly different picture. However, every internal auditor today should have at least a CBOK level of knowledge of the topics discussed in these chapters.

Note

1. Institute of Internal Auditors Research Foundation, *A Global Summary of the Common Body of Knowledge* (Altamonte Springs, FL, 2006). The IIARF issued both a preview and a final edition in 2008.

Index

Access to All Internal Audit Reports
  Audit Committee Responsibilities for Internal Audit, 541
ACL CAATT Programming Example
  Types of CAATTs, 492
ACL Continuous Assurance Auditing System
  Continuous Assurance Auditing (CAA) Processes, 650
Administrative Files
  Workpaper Document Organization, 341
AICPA Internal Control Research
  Cohen Commission, 28
AICPA SAS No. 1
  Controls Standards Background, 25
AICPA SAS No. 99
  Association of Certified Fraud Examiners (ACFE), 577
  Public Accounting's Role in Fraud Detection, 577
Application Controls
  Control Activities, 27
Application Controls Reviews
  Application Review Client-Server Budgeting System Example, 449
  Application Tests of Compliance, 451
  Computer-Assisted Audit Tool & Techniques (CAATT) Processes, 447
  Continuous Audit Monitoring Approaches, 447
  Functional Design Specifications, 438
  Internal Audit Report Findings, 426
  IT Application Audit Test Procedures, 445
  IT Applications Development Reviews, 433
  Purchased Software Internal Controls Audit Checklist, 435
  Reimplementation Internal Audit Reviews, 433
  Systems Development Methodology (SDM) Processes, 438
Application Review Client-Server Budgeting System Example
  Application Controls Reviews, 449
  Capital Budgeting Application Input and Output Audit Tests, 450
Application Tests of Compliance
  Application Controls Reviews, 451
Application Walk-Throughs
  Internal Auditor Steps, 439
Applications for Internal Audit Reviews
  Control Risk Considerations, 436
AS 5 Key Concepts
  Risk Management, 113
AS 5 Rules
  Internal Audit Competence and Objectivity Assessments, 86
  Internal Audit Roles, 84
ASQ Internal Audit Certifications
  Certified Quality Auditor (CQA) Requirements, 626
  Professional Certifications, 625
ASQ Quality Audit Division (QAD)
  Classifications of Quality Audits, 681
  Quality Auditor Duties and Responsibilities, 680
Assignment of Authority and Responsibility
  Control Environment, 37
  Enterprise Objectives, 37
Association of Certified Fraud Examiners (ACFE)
  AICPA SAS No. 99, 577
Attribute Sampling Parameters
  Attributes Sampling, 217
Attributes Sampling
  Advantages and Limitations, 224
  Attribute Sampling Parameters, 217
  Attributes Sampling Test Example, 221
  Audit Sampling Approaches, 216
  SOx Section 404 Internal Controls Tests, 216
Attributes Sampling Test Example
  Attributes Sampling, 221

Audit and Consulting Separation of Duties
Internal Audit as an Enterprise Consultant, 633
Audit Assessment and Evaluation Techniques
Performing an Individual Internal Audit, 200
Audit Bulk Files
Workpaper Standards, 344
Audit Committee Approvals
Internal Audit Internal Consulting Capabilities, 631
Audit Committee Charters
Microsoft Corporation's 2007 Audit Committee Charter, 536
Audit Committee Expanded Responsibilities
Internal Audit Key Competencies, 533
Audit Committee Financial Expert
Internal Audit Support Roles, 539
Audit Committee Financial Expert Rules
SEC Audit Committee Rules, 537
Audit Committee Formal Whistleblower Programs
SOx Requirements, 547
Audit Committee Governance
SEC Audit Committee Rules, 533
Audit Committee Organization and Charters
Corporate Governance, 533
Internal Audit Charters, 535
NYSE Model Audit Committee Charter, 535
Audit Committee Preapproval of Services
SOx Title II: Auditor Independence, 61
Audit Committee Responsibilities for Internal Audit
Access to All Internal Audit Reports, 541
Chief Audit Executive (CAE) Appointment, 541
Internal Audit Charter Approval, 542
Internal Audit Health Check Assessment, 540
Internal Audit Plan and Budget Approvals, 543
Audit Committee Review and Action
Significant Internal Audit Findings, 545
Audit Committee Roles and Responsibilities
Internal Audit Key Competencies, 532, 546
Internal Auditor CBOK Requirements, 531
Whistleblower Responsibilities, 546
Audit Evidence
Audit Sampling, 200
Evidence Classifications, 251
Performing an Individual Internal Audit, 199
Audit Evidence Gathering
CAATT Procedures, 503
Audit Evidence Types
IIA Professional Standards, 171
Audit Exit or Closing Conferences
Reporting Internal Audit Results, 370
Audit Fieldwork
Preliminary Findings Point Sheets, 328
Audit Findings
Preliminary Audit Findings, 177
Audit Findings Problems
Judgmental Sampling, 204
Audit Focal Points
Planning Internal Audit Activities, 239
Audit Plan Project Schedule Example
Organizing and Planning Internal Audits, 156
Audit Plan Summary for Audit Committee Review
Internal Audit Plan and Budget Approvals, 544
Audit Procedures Files
Workpaper Document Organization, 342
Audit Program Checklists
Audit Program Formats, 249
Audit Program Formats
Audit Program Checklists, 249
Audit Programs
Checklist Format Audit Programs, 170
Internal Audit Activity Plans, 247
Internal Audit Planning, 166
Procedure Oriented Audit Programs, 171
Audit Quality Control Standards
ISO 9000, 58
SOx Title I: Public Company Accounting Oversight Board, 58
Audit Report and Workpaper Retention
Document Backup, Security, and Continuity, 372
Audit Report Findings
Audit Report Formats, 358
Audit Report Formats
Audit Report Findings, 358
Audit Report Presentation Guidelines, 362
Auditor's Opinions, 355
Draft Audit Reports, 368
Final Audit Report Example, 369
Informal Memo Format Audit Reports, 356

Internal Audit Reports, 353
Oral or Informal Audit Reports, 365
Questionnaire-Format Audit Reports, 366
Audit Report Preparation Steps
Internal Audit Reporting Cycle, 366
Audit Report Presentation Guidelines
Audit Report Formats, 362
Audit Report Recommendations
Internal Audit Key Competencies, 301
Audit Reports
Basic Objectives and Components, 352
Audit Reports and Privacy
Security and Privacy in the Internal Audit Department, 477
Audit Sampling
Audit Evidence, 200
Internal Auditor CBOK Requirements, 201, 233
Judgmental Sampling, 203
Monetary Unit Sampling, 225
Statistical Sampling Concepts, 205
Statistical Sampling Plans, 210
Audit Sampling Approaches
Attributes Sampling, 216
Bayesian Sampling, 233
Multistage Sampling, 232
Replicated Sampling, 232
Variables Sampling, 215
Audit Scheduling and Time Estimates
Internal Audit Planning, 158
Audit Universe Maintenance
Internal Audit Activity Plans, 252
Auditable Activities
Internal Audit Universe, 238
Auditing a Business Continuity Plan (BCP)
Internal Audit Review Points, 520
Auditing Applications under Development
Objectives and Obstacles of Reimplementation Auditing, 452
Performing Applications Controls Reviews, 451
Reimplementation Review Objectives, 453
Reimplementation Review Problems, 454
Reimplementation Review Procedures, 455
Auditing Business Continuity Planning Processes
Centralized Data Center BCP Reviews, 508
Sarbanes-Oxley Act (SOx), 508
Auditing Business Continuity Plans
IT Disaster and Business Continuity Planning, 526
Auditing COSO ERM
Internal Audit Procedures, 148
Auditing IT Costs and Pricing
ITIL Service Delivery IT Financial Management, 419
Auditing IT General Controls
Auditing IT Infrastructure Management, 422
Characteristics of Larger IT Systems, 394
Client-Server and Smaller IT Systems, 390
Compliance with Laws or Regulations, 403
IT System Update Controls, 392
Large System IT General Controls Objectives, 403
Legacy System General Controls Reviews, 400
Mainframe and Legacy Systems, 394
Auditing IT Infrastructure Management
Auditing IT General Controls, 422
Auditing IT Security and Privacy
Cybersecurity Internal Controls Audit Procedures, 473
Internal Audit Key Competencies, 472
Reviews of IT and Cybersecurity Controls, 472
Auditing Six Sigma Processes
Internal Audit Procedures, 718
Internal Audit Procedures for a Review of a Six Sigma Program, 720
Auditing Standard No. 5 (AS, 5)
Sarbanes-Oxley Act Key Provisions, 57
Auditing the Enterprise's Ethics Functions
Ethics and Whistleblower Programs, 568
Auditor Prepared Test Files
Types of CAATTs, 495
Auditor's Opinions
Audit Report Formats, 355
Authorizing Internal Audit Internal Consulting
Audit Charters, 634
Automated Purchasing System Compliance Tests
Performing Applications Controls Reviews, 447

Background and History
CobiT, 90
Background of the IIA Standards
International Standards for the Professional Practice of Internal Auditing, 184
Baldridge National Quality Award
Six Sigma Background and Concepts, 708

Basic Accounting Cycles
Section 404 Compliance Reviews, 76
Basic CobiT Principles
CobiT Framework, 93
Basic Objectives and Components
Audit Reports, 352
Basic Understandings of the General Use of CAATTs
CAATT Software Tools, 487
Determining the Need for CAATTs, 484
Internal Auditor CBOK Requirements, 481, 503
Selecting Appropriate CAATT Processes, 501
Bayesian Sampling
Audit Sampling Approaches, 233
BCP Client-Server Readiness Review
Internal Audit Procedures, 514
BCP Contingency Strategies
Data Mirroring Techniques, 524
Fully Mirrored Recovery Operations, 519
High-Availability Percentage Parameters, 525
Switchable Hot Site Facilities, 519
Traditional Hot Sites, 519
BCP Risk and Business Impact Analysis
IT Business Continuity Plans, 517
BCP Training
IT Disaster and Business Continuity Planning, 523
Benchmarking
IIA "Progress through Sharing" Motto, 265
Independent Internal Control Evaluations, 48
Internal Audit Roles, 262
Internal Auditor CBOK Requirements, 253
Black Belt Body of Knowledge
Six Sigma Background and Concepts, 712
Board of Directors and Audit Committee
Control Environment, 36
Board Resolutions an Audit Committee
Corporate Governance, 534
Book Objective
Modern Internal Auditing, 3
Bribery Restrictions
Foreign Corrupt Practices Act of 1977 (FCPA), 27
Building an Effective Internal Audit Function
Internal Audit Best Practices, 273
Building Effective CAATTs
CAATT Procedures, 501
Business Continuity Planning
Service-Level Agreements (SLAs), 523
Business Continuity Planning Key Steps
Disaster Recovery Institute, 509
Business Criticality Outage Impact Analysis
IT Business Continuity Plans, 518
Business Requirements Components
CobiT Cube, 95

CAA Benefits
Continuous Assurance Auditing (CAA) Processes, 651
CAATT Document Repositories
Workpaper Review Processes, 349
CAATT History and Background
Equity Funding Fraud, 482
CAATT Procedures
Audit Evidence Gathering, 503
Building Effective CAATTs, 501
Comparing Data across Separate Files, 486
Examining Records Based on Criteria Specified by Internal Audit, 486
Selecting and Printing Audit Samples, 487
Testing Calculations and Making Computations, 486
CAATT Software Tools
Basic Understandings of the General Use of CAATTs, 487
CAATT Types
ACL CAATT Programming Example, 492
Auditor Prepared Test Files, 495
Desktop and Laptop CAATTs, 491
Embedded Audit Procedures, 496
Generalized Audit Software, 488
Report Generators Languages, 489
Specialized Audit Test and Analysis Software, 496
Test Deck Approaches, 492
Capability Maturity Model (CMMi)
CobiT Monitoring and Evaluation Processes, 107
Capital Budgeting Application Input and Output Audit Tests
Application Review Client-Server Budgeting System Example, 450
Cause-and-Effect Diagram
Implementing Consulting Recommendations, 639
CBOK for the Modern Internal Auditor
Internal Auditor Needs for a Common Body of Knowledge (CBOK), 731

CBOK Level of General Understanding Requirements
ISO Standards and Internal Auditors, 678
CBOK Objectives
Internal Auditor Knowledge Requirements, 19
Standards for the Professional Practice of Internal Auditing, 18
CBOK Requirements
COSO Internal Controls Framework, 24
CCSA® Requirements
Certified Control Self-Assessment Examination Topics, 617
CIA-Related Professional Certifications, 615
Centralized Data Center BCP Reviews
Auditing Business Continuity Planning Processes, 508
Centralized IT Facilities
Internal Audit BCP Review Procedures, 511
Certification in Control Self-Assessment (CCSA)
IIA CSA Methodology, 262
Certified Control Self-Assessment Examination Topics
CCSA® Requirements, 617
Certified Fraud Examiner (CFE) Certification
Professional Certifications, 623
Certified Government Audit Professional Examination Topics
CGAP® Requirements, 618
Certified Information Security Manager® (CISM) Certification
Professional Certifications, 622
Certified Information Systems Auditor (CISA) Requirements
CISA Examination Content Areas, 622
Professional Certifications, 619
Certified Information Systems Security Professional (CISSP) Certification
Professional Certifications, 624
Certified Internal Auditor Responsibilities and Requirements
CIA Examination, 608
Professional Certifications, 606
Certified Quality Auditor (CQA) Requirements
ASQ Internal Audit Certifications, 626
CFSA® Requirements
CIA Examination Summary, 619
CGAP® Requirements
Certified Government Audit Professional Examination Topics, 618
CIA-Related Professional Certifications, 616
Characteristics of Larger IT Systems
Auditing IT General Controls, 394
Operating Systems Software, 398
Checklist Format Audit Programs
Audit Programs, 170
Chief Audit Executive (CAE) Appointment
Audit Committee Responsibilities for Internal Audit, 541
Chief Audit Executive (CAE) Overall Workpaper Responsibility
Workpaper Review Processes, 347
Chief Audit Executive (CAE) Roles
Establishing an Internal Audit Function, 277
CIA Examination
Certified Internal Auditor Responsibilities and Requirements, 608
CIA Examination Summary, 608
CIA Examination Summary
CFSA® Requirements, 619
CIA Examination, 608
Internal Auditor CBOK Requirements, 608
CIA Responsibilities and Requirements
Professional Certifications, 606
CIA-Related Professional Certifications
CCSA® Requirements, 615
CGAP® Requirements, 616
CISA Examination Content Areas
Certified Information Systems Auditor (CISA) Requirements, 622
Classifications of Quality Audits
ASQ Quality Audit Division (QAD), 681
Types of Quality Audits, 682
Client-Server and Smaller IT Systems
Auditing IT General Controls, 390
Client-Server System Configuration, 387
IT Control Risks, 389
IT General Controls, 383
Client-Server and Web-Based Applications
IT Disaster and Business Continuity Planning, 507
Client-Server Continuity Planning Internal Audit Procedures
IT Disaster and Business Continuity Planning, 513
Client-Server System Configuration
Client-Server and Smaller IT Systems, 387
Cluster Selection Sampling
Statistical Sampling Plans, 213

CobiT
Background and History, 90
CobiT Assurance Framework Guidance, 110
Information Systems Audit and Control Association (ISACA), 90
Internal Auditor CBOK Requirements, 111
Internal Controls Reviews, 96
IT Assurance Framework (ITAF), 110
IT Governance Focus Areas, 91
IT Governance Institute (ITGI), 90
Navigating the CobiT Framework, 97
SOx Section 404 Internal Controls Assessments, 90
SOx Section 404 Internal Controls Assessments, 108
CobiT Acquisition and Implementation Processes
CobiT Navigation, 100
CobiT Assurance Framework Guidance
CobiT, 110
CobiT Cube
Business Requirements Components, 95
CobiT Framework, 93
CobiT Cube Components
CobiT Domain Areas, 95
IT Processes, 95
IT Resources, 94
CobiT Delivery and Support Processes
CobiT Navigation, 102
CobiT Domain Areas
CobiT Cube Components, 95
Systems Development Life Cycle (SDLC) Procedures, 95
CobiT Framework
Basic CobiT Principles, 93
CobiT Cube, 93
CobiT Monitoring and Evaluation Processes
Capability Maturity Model (CMMi), 107
CobiT Navigation, 103
COSO Components and CobiT Objectives, 107
Deming's PDCA Cycle, 105
Edward Deming Quality Systems Approaches, 104
CobiT Navigation
CobiT Acquisition and Implementation Processes, 100
CobiT Delivery and Support Processes, 102
CobiT Monitoring and Evaluation Processes, 103
CobiT Planning and Enterprise Processes, 98
CobiT Objectives
RACI Chart Responsibilities, 99
CobiT Planning and Enterprise Processes
CobiT Navigation, 98
COBOL Programming Language Example
Computer Programming Languages, 431
Code of Conduct Knowledge and Compliance
Internal Auditor CBOK Requirements, 550
Code of Conduct Revisions
Enterprise Codes of Conduct, 561
Code of Conduct Violations and Corrective Actions
Enterprise Codes of Conduct, 560
Code of Ethics
Information Systems Audit and Control Association (ISACA), 198
The Institute of Internal Auditors (IIA), 197
Integrity and Ethical Values, 34
Codes of Conduct
Ethical Behavior Rules, 34
Codes of Conduct Contents
Enterprise Codes of Conduct, 557
Cohen Commission
AICPA Internal Control Research, 28
Financial Executives International (FEI), 29
Commitment to Competence
Control Environment, 35
COSO ERM Internal Environment, 128
Committee of Sponsoring Organizations (COSO)
Internal Controls Definition, 23
Common Body of Knowledge (CBOK)
Definition of a CBOK, 11
IIARF CBOK Survey, 13
Institute of Internal Auditors Research Foundation (IIARF), 13
Internal Auditing Origins, 11
Communications
COSO Internal Control Elements, 45
Communications and Information
Communications: Internal Components, 30
COSO Internal Controls Framework, 28
COSO Internal Controls Framework, 43
External Communications, 31
Methods of Communication, 32
Quality of Information, 29
Strategic and Integrated Systems, 29
Whistleblower Programs, 45
Communications from External Parties
Monitoring, 47

Communications: Internal Components
Communications and Information, 30
Comparing Data Across Separate Files
CAATT Procedures, 486
Compliance and Governance Requirements
HIPAA: Healthcare Related Rules, 588
Compliance with IIA Standards
IIARF CBOK Evaluation Results, 15
Compliance with Laws or Regulations
Auditing IT General Controls, 403
Computer Forensics
IT Fraud Prevention Processes, 584
Computer Programming Languages
COBOL Programming Language Example, 431
Object-Oriented Programming Language Concepts, 432
Computer-Aided Systems Engineering (CASE) Software Tools
Specialized Audit Test and Analysis Software, 496
Computer-Assisted Audit Tool & Techniques (CAATT) Processes
Application Controls Reviews, 447
Computer-Assisted Audit Tools and Techniques
Internal Audit Key Competencies, 481
Concurring Partner Approvals
SOx Title I: Public Company Accounting Oversight Board, 58
Consulting Best Practices
Consulting Engagement Letters, 638
Documenting and Completing the Consulting Engagement, 640
Internal Audit Internal Consulting Capabilities, 635
Internal Auditor CBOK Requirements, 630
Launching a Consulting Assignment, 636
Consulting Engagement Letters
Consulting Best Practices, 638
Continuing Education Requirements
Internal Auditor Commitment to Learning, 304
Continuity Planning for Desktop and Laptop Applications
IT Disaster and Business Continuity Planning, 513
Continuous Assurance Auditing (CAA) Processes
ACL Continuous Assurance Auditing System, 650
CAA Benefits, 651
Continuous Assurance Auditing Conceptual Model, 647
Dashboard Monitoring Systems, 650
Implementing Continuous Assurance Auditing, 644
Continuous Assurance Auditing Conceptual Model
Continuous Assurance Auditing (CAA) Processes, 647
Continuous Audit Monitoring Approaches
Application Controls Reviews, 447
Continuous Audit Monitoring Processes
Data Mining, and OLAP, 655
Data Warehouses, 655
Online Analytical Processing (OLAP), 658
Payment System Continuous Audit Monitor, 646
Continuous Audit Monitors
Embedded Audit Procedures, 497
Continuous Close Processes
SOx Closing Requirements, 659
Control Activity Types
COSO Internal Controls Framework, 41
Control Activities
Application Controls, 27
COSO ERM Framework, 138
COSO ERM Risk Event Identification, 138
COSO Internal Controls Framework, 24
ERM Policies and Procedures, 138
IT Controls, 27
Risk Assessment Processes, 26
Control Environment
Assignment of Authority and Responsibility, 37
Board of Directors and Audit Committee, 36
Commitment to Competence, 35
COSO Internal Control Foundation Components, 38
COSO Internal Controls Framework, 33
Human Resources Policies and Practices, 37
Integrity and Ethical Values, 34
Management's Philosophy and Operating Style, 36
Organizational Structure, 36
Tone at the Top, 34
Control Risk Considerations
Applications for Internal Audit Reviews, 436
Control Self-Assessments
CSA Process, 255
Evaluating CSA Results, 261
IIA CSA Methodology, 254

Control Self-Assessments (*Continued*)
Internal Auditor CBOK Requirements, 253
International Standards for the Professional Practice of Internal Auditing, 254
Controls Definition
Standards for the Professional Practice of Internal Auditing, 25
Controls Standards Background
AICPA SAS No. 1, 25
Securities Exchange Act of 1934, 25
Corporate Governance
Audit Committee Organization and Charters, 533
Board Resolutions an Audit Committee, 534
COSO
Internal Controls Definition, 23
COSO and CobiT Relationships
Mapping Internal Control Frameworks, 109
COSO Components and CobiT Objectives
CobiT Monitoring and Evaluation Processes, 107
COSO Definition of Internal Controls
Internal Controls, 24
COSO Enterprise Risk Management (COSO ERM)
Risk Assessments, 113
COSO ERM
Enterprise Risk Management, 124
Internal Auditor CBOK Requirements, 114, 146
Risk Management Fundamentals, 114
COSO ERM Framework
Control Activities, 138
COSO ERM Information and Communication, 140
COSO ERM Key Elements, 126
COSO ERM Monitoring, 141
Entity-Level Risks, 145
Legal and Regulatory Compliance Risk Objectives, 143
Operations Risk Management Objectives, 142
Reporting Risk Management Objectives, 143
Risk Management Philosophy, 127
COSO ERM Information and Communication
COSO ERM Framework, 140
COSO ERM Internal Environment
Commitment to Competence, 128
Risk Appetite, 128
Risk Event Identification, 132
Risk Management Philosophy, 127
Risk Objective Setting, 130
COSO ERM Key Elements
COSO ERM Framework, 126
COSO ERM Monitoring
COSO ERM Framework, 141
COSO ERM Risk Event Identification
Control Activities, 138
ERM Control Activities, 139
SOx Section 404 Requirements, 138
COSO Internal Control Definition
COSO Internal Controls Framework, 32
COSO Internal Control Elements
Communications, 45
COSO Internal Control Foundation Components
Control Environment, 38
COSO Internal Controls Framework, 39
COSO Internal Control Framework
Treadway Committee Report, 31
COSO Internal Controls
Internal Controls Definition, 24
COSO Internal Controls Framework
CBOK Requirements, 24
Importance of Internal Controls, 24
Internal Controls Importance, 24
SOx Section 404 Internal Controls Assessments, 76
Communications and Information, 28, 43
Control Activities, 24
Control Environment, 33
COSO Internal Control Definition, 32
COSO Internal Control Foundation Components, 39
Independent Internal Control Evaluations, 48
Integration of Control Activities with Risk Assessment, 42
Internal Audit CBOK Requirements, 51
Internal Control Definitions, 31
Internal Control Evaluation Processes, 48
IT Controls, 42
Monitoring, 32, 46
Quality of Information, 44
Reporting Internal Control Deficiencies, 48
Risk Assessment, 23, 39
Risk Assessment Process, 23
Strategic and Integrated Systems, 44
Types of Control Activities, 41
Unethical, Illegal, or Otherwise Improper Activities, 45

Credit Card Fraud
GLBA Pretexting Provisions, 599
Identity Theft and Assumption Deterrence Act, 600
Cryptography, PKI, and HIPAA Security Requirements
HIPAA: Healthcare related Rules, 591
CSA Facilitated Sessions
Performing Facilitated CSA Reviews, 258
CSA Process
Control Self-Assessments, 255
CSA Review Approaches
Facilitated Team Meetings, 257
CSA Reviews
Enterprise Control Environment Improvements, 256
Enterprise Resource Planning (ERP) Systems, 256
Cybersecurity and Privacy Controls
Internal Audit's Privacy and Cybersecurity Roles, 479
PCI-DSS Requirements, 478
Cybersecurity Internal Controls Audit Procedures
Auditing IT Security and Privacy, 473
Cybersecurity Risks and Controls
Internal Auditor CBOK Requirements, 461
IT Network Security Fundamentals, 462
IT Systems Privacy Concerns, 469
Security and Privacy in the Internal Audit Department, 474

Dashboard Monitoring Systems
Continuous Assurance Auditing (CAA) Processes, 650
Data Mining, and OLAP
Continuous Monitoring Processes, 655
Data Mirroring Techniques
BCP Contingency Strategies, 524
Data Profiling Issues
IT Systems Privacy Concerns, 469
Data Warehouse Transformation Example
Data Warehouses, 657
Data Warehouses
Continuous Monitoring Processes, 655
Data Warehouse Transformation Example, 657
Definition of a CBOK
Common Body of Knowledge (CBOK), 11
PMI's PMBOK, 12
Definition of a Fraud
Reasons for Committing Fraud, 576
Definition of Internal Controls
Internal Controls, 24
Deming's PDCA Cycle
CobiT Monitoring and Evaluation Processes, 105
Desktop and Laptop CAATTs
Types of CAATTs, 491
Desktop and Laptop Systems BCP Processes
Internal Audit Procedures, 515
Determine the Audit Objectives
Internal Audit Planning, 157
Determining the Need for CAATTs
Basic Understandings of the General Use of CAATTs, 484
Developing a CAATT Application
Generalized Audit Software, 489
Developing a Project Management Plan
Project Management, 310
Developing and Preparing Audit Programs
Internal Audit Planning, 166
Developing Application Control Objectives
Performing Applications Controls Reviews, 442
Developing Appropriate Internal Audit Procedures
Planning and Performing Internal Audits, 324
Developing Effective Internal Audit Recommendations
Internal Auditor CBOK Requirements, 377
Developing Preliminary Internal Audit Plans
Internal Audit Key Competencies, 323
Disaster Recovery Emergency Handling
IT Disaster and Business Continuity Planning, 522
Disaster Recovery Institute
Business Continuity Planning Key Steps, 509
DMAIC Procedures for a Six Sigma Project
Six Sigma Design-Measure-Analyze-Improve-Control (DMAIC) Model, 715
Document Backup, Security, and Continuity
Audit Report and Workpaper Retention, 372
Laptop-Based Internal Audit Systems, 348
Workpaper Review Processes, 348
Document Standards and Review Processes
Workpaper Review Processes, 348
Documenting the Internal Controls Environment
Internal Audit Key Competencies, 323

Documenting and Completing the Consulting Engagement
Consulting Best Practices, 640
Documenting Internal Audit Results
Internal Audit Workpapers, 335
Laptop Computers, 340
Process Model Example, 331
Process Modeling and Workpapers, 329
Process Modeling Hierarchy, 333
Workpaper Document Organization, 340
Workpaper Objectives, 336
Documenting the Internal Audit Field Surveys
Internal Audit Planning, 164
Workpaper Permanent Files, 166
Draft Audit Reports
Audit Report Formats, 368
Due Professional Care
Internal Audit Attribute Standards, 189, 190

Edward Deming Quality Systems Approaches
CobiT Monitoring and Evaluation Processes, 104
Effective Internal Audit Communications
Reporting Internal Audit Results, 374
Effective Internal Audit Plans
Project Management, 318
Effective Risk Management Processes
Risk Management Fundamentals, 115
Embedded Audit Procedures
Continuous Audit Monitors, 497
Integrated Test Facilities (ITFs), 499
Types of CAATTs, 496
Emergency Response Plans
IT Disaster and Business Continuity Planning, 512
Engagement Letters
Internal Audit Planning, 161
Engagement Planning
Internal Audit Performance Standards, 193
Enterprise Codes of Conduct
Code of Conduct Contents, 557
Code of Conduct Revisions, 561
Code of Conduct Violations and Corrective Actions, 560
Ethics and Whistleblower Programs, 557
SOx Title IV: Enhanced Financial Disclosures, 71
Enterprise Consulting Activities
International Standards for the Professional Practice of Internal Auditing, 629
Enterprise Control Environment Improvements
CSA Reviews, 256
Enterprise Help or Hotline Functions
Ethics and Whistleblower Programs, 564
Enterprise Objectives
Assignment of Authority and Responsibility, 37
Enterprise Resource Planning (ERP) Systems
CSA Reviews, 256
Enterprise Risk Management
COSO ERM, 124
Enterprise Risk Objectives
Legal and Regulatory Compliance Requirements, 143
Enterprise Risks
Risk Identification, 117
Enterprise-Wide Strategic Risks
Risk Identification, 117
Entity-Level Risks
COSO ERM Framework, 145
e-Office Documentation Best Practices
Internal Auditor Documentation, 299
Equity Funding
IT Auditing Background, 382
Equity Funding Fraud
CAATT History and Background, 482
ERM Control Activities
COSO ERM Risk Event Identification, 139
ERM Policies and Procedures
Control Activities, 138
Establishing an Internal Audit Function
Chief Audit Executive (CAE) Roles, 277
Internal Audit Position Descriptions, 279
Internal Audit Charters, 275
Internal Audit Management Responsibilities, 278
Internal Audit Organization Approaches, 283
Internal Audit Policies and Procedures, 290
International Standards for the Professional Practice of Internal Auditing, 274
Ethical Behavior Rules
Code of Conduct, 34
Ethics and Whistleblower Programs
Auditing the Enterprise's Ethics Functions, 568
Enterprise Codes of Conduct, 557

Enterprise Help or Hotline Functions, 564
Ethics Environment Attitude Surveys, 555
Ethics Risk Environments, 553
Internal Audit Key Competencies, 549
Mission Statements, 551
SOx Whistleblower Call Center Guidelines, 565
Whistleblower and Hotline Functions, 562
Ethics Environment Attitude Surveys
Ethics and Whistleblower Programs, 555
Summarizing Ethics Survey Results, 556
Ethics Risk Environments
Ethics and Whistleblower Programs, 553
Evaluating CSA Results
Control Self-Assessments, 261
Evaluating Monetary Unit Sample Results
Monetary Unit Sampling, 228
Evidence Classifications
Audit Evidence, 251
Examining Records Based on Criteria Specified by Internal Audit
CAATT Procedures, 486
Expectations Gap Auditing Standards
Financial Auditing Standards, 30
External Audit Conflicts of Interest
SOx Title II: Auditor Independence, 62
External Communications
Communications and Information, 31
External Factor Risks
Risk Assessment Processes, 23

Facilitated Team Meetings
CSA Review Approaches, 257
Failures to Detect Fraud
Fraud Detection and Prevention, 574
FCPA Aftermath
Foreign Corrupt Practices Act of 1977 (FCPA), 27
FCPA Record-keeping Requirements
Foreign Corrupt Practices Act of 1977 (FCPA), 27
Final Audit Report Example
Audit Report Formats, 369
Financial Accounting Standards Board (FASB)
PCAOB Accounting Standards Authority, 59
Financial and Business Reporting Tools
XBRL: Internet-Based Extensible Business Reporting Language, 651
Financial Auditing Standards
Expectations Gap Auditing Standards, 30
SAS No. 55, 30
Financial Executives International (FEI)
Cohen Commission, 29
Financial Information Systems Design
Public Accounting Firm Prohibitions, 61
Financial Officer Codes of Conduct
SOx Title IV: Enhanced Financial Disclosures, 70
Financial Reporting Standards Convergence
International Financial Reporting and Auditing Standards as of January 2008, 725
Foreign Corrupt Practices Act of 1977 (FCPA)
Bribery Restrictions, 27
FCPA Aftermath, 27
FCPA Record-Keeping Requirements, 27
Internal Accounting Controls Requirements, 27
Internal Control Definitions, 26
Slush Funds, 27
Foundations of Internal Auditing
Mesopotamian Civilizations, 3
Fraud Detection and Prevention
Failures to Detect Fraud, 574
Internal Audit Key Competencies, 571
Internal Auditor CBOK Requirements, 585
IT Fraud Prevention Processes, 583
Practice of Internal Auditing, 585
Red Flags Indicating Potential Financial Fraud, 574
Understanding and Recognizing Fraud, 572
Fraud Investigations
Internal Audit Roles and Responsibilities, 580
Fraud Risk Factors
Misappropriation of Assets, 579
Fully Mirrored Recovery Operations
BCP Contingency Strategies, 519
Functional Design Specifications
Application Controls Reviews, 438
Future Directions for Quality-Assurance Auditing, 704

GAIN Annual Benchmarking Study
Global Audit Information Network (GAIN), 265
General Control Objectives
Smaller Business IT Systems, 393
Generalized Audit Software
Developing a CAATT Application, 489
Types of CAATTs, 488

GLBA Financial Privacy Rules
Gramm-Leach-Bliley Act (GLBA), 596
GLBA Pretexting Provisions
Credit Card Fraud, 599
Gramm-Leach-Bliley Act (GLBA), 599
GLBA Safeguards Rule Compliance
Internal Audit Review Focus Areas, 598
GLBA-Mandated Privacy Requirements
Gramm-Leach-Bliley Act (GLBA), 597
Global Audit Information Network (GAIN)
GAIN Annual Benchmarking Study, 265
Internal Audit Best Practices, 265
Global Computer Products Example Company
Key Characteristics, 240
Sample Organization Chart, 242
Gramm-Leach-Bliley Act (GLBA)
GLBA Financial Privacy Rules, 596
GLBA Pretexting Provisions, 599
GLBA-Mandated Privacy Requirements, 597
Internal Audit Rules, 595
Gramm-Leach-Bliley Compliance
Internal Audit Procedures, 601

High-Availability Percentage Parameters
BCP Contingency Strategies, 525
HIPAA Patient Record Privacy Rules
HIPAA: Healthcare related Rules, 589
HIPAA Primary Objectives
HIPAA: Healthcare related Rules, 589
HIPAA Privacy Administration
HIPAA: Healthcare related Rules, 590
HIPAA Required Implementation Specifications
HIPAA Security Administrative Procedures, 593
HIPAA Security Administrative Procedures
HIPAA Required Implementation Specifications, 593
HIPAA: Healthcare Related Rules
Compliance and Governance Requirements, 588
Cryptography, PKI, and HIPAA Security Requirements, 591
HIPAA Patient Record Privacy Rules, 589
HIPAA Primary Objectives, 589
HIPAA Privacy Administration, 590
Internal Audit HIPAA Requirements Procedures, 592
Technical Security Services and Mechanisms, 594

Histograms
Statistical Sampling Concepts, 207
History of Internal Auditing
Internal Audit Responsibilities, 7
Internal Auditing, 4
Victor Z. Brink, 5
Human Resources Policies and Practices
Control Environment, 37

Identity Theft and Assumption Deterrence Act
Credit Card Fraud, 600
IIA
Origins—First Membership Chapter, 5
IIA "Progress through Sharing" Motto
Benchmarking, 265
IIA CBOK Needs
IIARF CBOK Survey Limitations, 17
IIA CSA Methodology
Certification in Control Self-Assessment (CCSA), 262
Control Self-Assessments, 254
IIA Definition
Modern Internal Auditing, 4
IIA GAIN Network
ISO Standards and Internal Auditors, 678
IIA Internal Auditors
Quality Audit Process Steps, 687
IIA Professional Standards
Audit Evidence Types, 171
IIA Standards Compliance
Management Agreements to IIARF CBOK Survey Results, 16
IIARF CBOK
IIARF CBOK Survey, 18
IIARF CBOK Evaluation Results
Compliance with IIA Standards, 15
Disturbing Observations, 15
Internal Audit Activity Adds Value to Governance Processes, 15
Internal Audit Brings Systematic Approaches to Evaluate Effectiveness, 15
Internal Audit Tools and Techniques, 16
Limitations/Problems with IIARF CBOK Survey, 15
Quality Management Techniques, 16
IIARF CBOK Survey
Common Body of Knowledge (CBOK), 13
Internal Auditing Activities (IAAs), 15
Objectives of IIARF CBOK, 14
Use of the IIARF CBOK, 18

IIARF CBOK Survey Limitations
IIA CBOK Needs, 17
Implementing Consulting Recommendations
Cause-and-Effect Diagram, 639
Implementing Continuous Assurance Auditing
Continuous Assurance Auditing (CAA) Processes, 644
Implementing Six Sigma
Six Sigma Background and Concepts, 709
Six Sigma Deployment and Process Guide, 710
Six Sigma Leadership Roles and Responsibilities, 711
Implementing XBRL
XBRL: Internet-Based Extensible Business Reporting Language, 653
Importance of Internal Controls
COSO Internal Controls Framework, 24
Importance of ISO Standards
International Organization for Standardization (ISO), 663
Independent Internal Control Evaluations
Benchmarking, 48
COSO Internal Controls Framework, 48
Independent Quality Assurance Reviews
International Standards for the Professional Practice of Internal Auditing, 186
Informal Memo Format Audit Reports
Audit Report Formats, 356
Information Systems Audit and Control Association (ISACA)
CobiT, 90
Code of Ethics, 198
Information Systems Audit Specialists
Internal Audit Position Descriptions, 281
Inherent Risk
Risk Assessment, 134
Input/Output Process Flowchart
Process Modeling for Internal Auditors, 334
Inspections, Investigations, and Disciplinary Procedures
SOx Title I: Public Company Accounting Oversight Board, 59
Institute of Internal Auditors
Origins—First Membership Chapter, 5
Institute of Internal Auditors Research Foundation (IIARF)
Common Body of Knowledge (CBOK), 13
Integrated Test Facilities (ITFs)
Embedded Audit Procedures, 499
Integration of Control Activities with Risk Assessment
COSO Internal Controls Framework, 42
Integrity and Ethical Values
Code of Ethics, 34
Control Environment, 34
Temptations that Encourage Improper Accounting, 35
Internal Factor Risks
Risk Assessment Processes, 23
Internal Accounting Controls Requirements
Foreign Corrupt Practices Act of 1977 (FCPA), 27
Internal Audit Position Descriptions
Establishing an Internal Audit Function, 279
Information Systems Audit Specialists, 281
Internal Audit Value to Governance Processes
IIARF CBOK Evaluation Results, 15
Internal Audit Activity Plans
Audit Programs, 247
Audit Universe Maintenance, 252
Internal Audit Universe, 238
Internal Audit Analytical Skills
Internal Audit Key Competencies, 296
Internal Audit as an Enterprise Consultant
Audit and Consulting Separation of Duties, 633
International Standards for the Professional Practice of Internal Auditing, 630
Internal Audit Attribute Standards
Due Professional Care, 189, 190
Internal Audit Charters, 188
International Standards for the Professional Practice of Internal Auditing, 188
IT Risks and Controls, 189
Quality Assurance and Improvement Programs, 190
Internal Audit BCP Review Procedures
Centralized IT Facilities, 511
Internal Audit Best Practices
Building an Effective Internal Audit Function, 273
Global Audit Information Network (GAIN), 265
Internal Audit Approaches to Evaluate Effectiveness
IIARF CBOK Evaluation Results, 15

Internal Audit CBOK Requirements
COSO Internal Controls Framework, 51
Internal Audit Charter Approval
Audit Committee Responsibilities for Internal Audit, 542
Internal Audit Charters
Audit Committee Organization and Charters, 535
Authorizing Internal Audit Internal Consulting, 634
Establishing an Internal Audit Function, 275
Internal Audit Attribute Standards, 188
Internal Audit Competence and Objectivity Assessments
AS 5 Rules, 86
Internal Audit Document Records Management
Workpaper Document Organization, 348
Internal Audit Documentation
Internal Auditor CBOK Requirements, 349
Internal Audit Documentation Requirements
Internal Auditor CBOK Requirements, 330
Workpaper Document Organization, 348
Internal Audit Field Surveys
Internal Audit Planning, 163
Internal Audit Fieldwork Procedures
Performing the Internal Audits, 173
Internal Audit Function
Quality Assurance Reviews, 688
Internal Audit Function Internal Quality Assurance Reviews
Internal Audit Quality-Assurance Review Benefits, 689
Internal Audit Quality-Assurance Review Elements, 689
Internal Audit Quality-Assurance Surveys, 702
International Standards for the Professional Practice of Internal Auditing, 688
Quality-Assurance Review of Internal Audit Review Steps, 699
Quality Review Engagement Letters, 696
Quality-Assurance Auditee Review Questions, 703
Quality-Assurance Review Approaches, 695
Internal Audit Health Check Assessment
Audit Committee Responsibilities for Internal Audit, 540
Internal Audit HIPAA Requirements Procedures
HIPAA: Healthcare related Rules, 592
Internal Audit Internal Consulting Capabilities
Audit Committee Approvals, 631
Consulting Best Practices, 635
Internal Audit Key Competencies
Quality Assurance Auditing (ASQ) Standards, 679
Analytical Skills, 296
Audit Committee Roles and Responsibilities, 532, 546
Audit Committees Expanded Responsibilities, 533
Audit Report Recommendations, 301
Auditing IT Security and Privacy, 472
Computer-Assisted Audit Tools and Techniques, 481
Developing Preliminary Internal Audit Plans, 323
Documenting the Internal Controls Environment, 323
Ethics and Whistleblower Programs, 549
Fraud Detection and Prevention, 571
Internal Auditor CBOK Requirements, 293
Internal Auditor Documentation, 298
Internal Auditor Interview Skills, 294
IT Application Controls, 425
Performing Applications Controls Reviews, 437
Project Management, 310
Project Management Best Practices, 319
Project Management Processes, 305
Internal Audit Management Responsibilities
Establishing an Internal Audit Function, 278
Internal Audit Objective Statements
Internal Audit Planning, 157
Internal Audit Objectives
Internal Audit Performance Standards, 193
Internal Audit Organization Approaches
Establishing an Internal Audit Function, 283
Internal Audit Performance Standards
Engagement Planning, 193
Internal Audit Objectives, 193
International Standards for the Professional Practice of Internal Auditing, 191
Risk Management, 192
Internal Audit Plan and Budget Approvals
Audit Committee Responsibilities for Internal Audit, 543
Audit Plan Summary for Audit Committee Review, 544

Internal Audit Planning
Audit Programs, 166
Audit Scheduling and Time Estimates, 158
Determine the Audit Objectives, 157
Developing and Preparing Audit Programs, 166
Documenting the Internal Audit Field Surveys, 164
Engagement Letters, 161
Internal Audit Field Surveys, 163
Internal Audit Objective Statements, 157
Preliminary Surveys, 159
Surprise Audits, 162
Internal Audit Policies and Procedures
Establishing an Internal Audit Function, 290
Internal Audit Practice Failure Observations
IIARF CBOK Evaluation Results, 15
Internal Audit Preparatory Activities
Performing Effective Internal Audits, 155
Internal Audit Procedures
Auditing COSO ERM, 148
Auditing Six Sigma Processes, 718
BCP Client-Server Readiness Review, 514
Desktop and Laptop Systems BCP Processes, 515
Gramm-Leach-Bliley Compliance, 601
IT Business Continuity Plans, 515
Quality-Assurance Review of Internal Audit, 691
Internal Audit Procedures for a Review of a Six Sigma Program
Auditing Six Sigma Processes, 720
Internal Audit Process Steps
Performing an Individual Internal Audit, 181
Internal Audit Quality-Assurance Review Benefits
Internal Audit Function Internal Quality-Assurance Reviews, 689
Internal Audit Quality-Assurance Review Elements
Internal Audit Function Internal Quality Assurance Reviews, 689
Internal Audit Quality-Assurance Surveys
Internal Audit Function Internal Quality Assurance Reviews, 702
Internal Audit Report Findings
Application Controls Reviews, 426
Internal Audit Reporting Cycle
Audit Report Preparation Steps, 366
Internal Audit Reports
Audit Report Formats, 353
Reporting Internal Audit Results, 351
Internal Audit Requirements
ISO 9001 on Quality Management Systems, 671
Internal Audit Responsibilities
History of Internal Auditing, 7
Internal Audit Review Focus Areas
GLBA Safeguards Rule Compliance, 598
Internal Audit Review Points
Auditing a Business Continuity Plan (BCP), 520
Internal Audit Roles
AS 5 Rules, 84
Benchmarking, 262
Performing a Benchmarking Study, 265
Performing Facilitated CSA Reviews, 257
Section 404 Compliance Reviews, 84
Service to Management, 8
Internal Audit Roles and Responsibilities
Fraud Investigations, 580
SOx Whistleblower Rules, 564
Internal Audit Rules
Gramm-Leach-Bliley Act (GLBA), 595
Internal Audit Scope and Objectives
Internal Audit Universe, 238
Internal Audit Self-Assessments
Preliminary Surveys, 159
Internal Audit Steps
ITIL Configuration Management, 412
Internal Audit Support Roles
Audit Committee Financial Expert, 539
Internal Audit Tools and Techniques
IIARF CBOK Evaluation Results, 16
Internal Audit Universe
Auditable Activities, 238
Internal Audit Activity Plans, 238
Internal Audit Scope and Objectives, 238
Internal Audit Workpapers
Documenting Internal Audit Results, 335
Internal Audit's Privacy and Cybersecurity Roles
Cybersecurity and Privacy Controls, 479
Internal Auditing
History of Internal Auditing, 4
Internal Auditing Activities (IAAs)
IIARF CBOK Survey, 15
Internal Auditing Definition
Modern Internal Auditing, 3
Internal Auditing History
Victor Z. Brink, 5
Internal Auditing Origins
Common Body of Knowledge (CBOK), 11

Internal Auditor CBOK Requirements
Audit Committee Roles and Responsibilities, 531
Audit Sampling, 201, 233
Basic Understandings of the General Use of CAATTs, 481
Basic Understandings of the General Use of CAATTs, 503
Benchmarking, 253
CIA Examination Summary, 608
CobiT, 111
Code of Conduct Knowledge and Compliance, 550
Consulting Best Practices, 630
Control Self-Assessments, 253
COSO ERM, 114, 146
Cybersecurity Risks and Controls, 461
Developing Effective Internal Audit Recommendations, 377
Fraud Detection and Prevention, 585
Internal Audit Documentation, 349
Internal Audit Documentation Requirements, 330
Internal Audit Key Competencies, 293
IT Application Controls, 426
IT General Controls, 381, 423
Organizing and Conducting a CSA Process, 262
Performing Effective Internal Audits, 153
Performing Effective QA Reviews, 705
Performing the Internal Audits, 172
Planning and Performing Internal Audits, 321
Process Modeling for Internal Auditors, 329
Six Sigma Principles, 721
Understanding Current IIA Standards, 183
Understanding HIPAA or GLBA Rules, 601
Understanding of BCP Requirements, 527
Understanding of Six Sigma Processes, 709
Internal Auditor Commitment to Learning
Continuing Education Requirements, 304
Internal Auditor Communication Skills, 304
Internal Auditor Communication Skills
Internal Auditor Commitment to Learning, 304
Internal Auditor Communication Skills, 302
Internal Auditor Negotiation Skills, 302
Testing and Analysis Skills, 296
Internal Auditor Documentation
e-Office Documentation Best Practices, 299
Internal Audit Key Competencies, 298
Internal Auditor General Understanding CBOK Needs
IT Systems Privacy Concerns, 470
Internal Auditor Independence
International Standards for the Professional Practice of Internal Auditing, 196
Internal Auditor Interview Skills
Internal Audit Key Competencies, 294
Internal Auditor Knowledge Needs
International Financial Reporting Standards (IFRS), 728
Internal Auditor Knowledge Requirements
CBOK Objectives, 19
Internal Auditor Needs for a Common Body of Knowledge (CBOK)
CBOK for the Modern Internal Auditor, 731
Internal Auditor Negotiation Skills
Internal Auditor Communication Skills, 302
Internal Auditor Outsourcing
SOx Title II: Auditor Independence, 60
Internal Auditor Steps
Application Walk-Throughs, 439
Internal Audit's Role
Section 404 Compliance Reviews, 78
Internal Control Definitions
COSO Internal Controls Framework, 31
Foreign Corrupt Practices Act of 1977 (FCPA), 26
Negative Assurance, 29
SAS No. 55, 30
Treadway Commission, 28
Treadway Committee Report, 31
Internal Control Evaluation Processes
COSO Internal Controls Framework, 48
Internal Control Evaluations
Monitoring, 34
Internal Control Structure in a Financial Statement Audit
SAS No. 55, 30
Internal Control Testing Scope
SOx Title I: Public Company Accounting Oversight Board, 58

Internal Controls
COSO Definition of Internal Controls, 24
Definition of Internal Controls, 24
Internal Controls Definition
Committee of Sponsoring Organizations (COSO), 23
COSO Internal Controls, 24
Internal Controls Importance
COSO Internal Controls Framework, 24
Internal Controls Reviews
CobiT, 96
International Accounting and Auditing Standards
U.S. Securities and Exchange Commission (SEC) Rules, 724
International Financial Reporting and Auditing Standards as of January, 2008
Financial Reporting Standards Convergence, 725
International Financial Reporting Standards (IFRS)
Internal Auditor Knowledge Needs, 728
U.S. Securities and Exchange Commission (SEC) Rules, 723
International Organization for Standardization (ISO)
Importance of ISO Standards, 663
International Standards for the Professional Practice of Internal Auditing
Background of the IIA Standards, 184
Control Self-Assessments, 254
Enterprise Consulting Activities, 629
Establishing an Internal Audit Function, 274
Independent Quality Assurance Reviews, 186
Internal Audit as an Enterprise Consultant, 630
Internal Audit Attribute Standards, 188
Internal Audit Function Internal Quality Assurance Reviews, 688
Internal Audit Performance Standards, 191
Internal Auditor Independence, 196
ISO International Internal Auditing Standards, 728
New Internal Audit Standards, 187
Organizing and Planning Internal Audits, 154
Practice of Internal Auditing, 580
Quality Assurance and Improvement Programs, 190
Red Book, 183
Workpaper Standards, 338
Internet Privacy Threats
IT Systems Privacy Concerns, 470
Radio Frequency Identification, 470
Interval Selection Sampling
Statistical Sampling Plans, 211
ISO, 15408
IT Security Evaluation Framework, 601
ISO 17799 and 27001 on IT Security
ISO Standards Overview, 672
ISO 19011 Auditing Principles
ISO 19011 on Quality Management Systems Auditing, 677
ISO 19011 on Quality Management Systems Auditing
ISO 19011 Auditing Principles, 677
ISO Standards Overview, 676
ISO 20000 on Service Quality Management:
ISO Standards Overview, 674
ISO 27001 Internal Audit Standards
Quality Auditor Duties and Responsibilities, 684
ISO 27001 on IT Security
IT Security Requirements, 674
ISO 27001 on Management Commitment
ISO Standards Example, 665
ISO 9000
Audit Quality Control Standards, 58
ISO 9001 on Quality Management Systems
Internal Audit Requirements, 671
ISO, 9001: 20000 Key Elements, 671
ISO Standards Overview, 667
Quality Management System Process, 669
ISO, 9001: 20000 Key Elements
ISO 9001 on Quality Management Systems, 671
ISO Documentation Hierarchy
ISO Standards, 669
ISO International Internal Auditing Standards
International Standards for the Professional Practice of Internal Auditing, 728
ISO Standards
ISO Documentation Hierarchy, 669
ITIL Best Practices, 665
ISO Standards and Internal Auditors
CBOK Level of General Understanding Requirements, 678
IIA GAIN Network, 678

ISO Standards Example
ISO 27001 on Management Commitment, 665
ISO Standards Overview
ISO 17799 and 27001 on IT Security, 672
ISO 19011 on Quality Management Systems Auditing, 676
ISO 20000 on Service Quality Management: 674
ISO 9001 on Quality Management Systems, 667
IT Assurance Framework (ITAF)
CobiT, 110
IT Application Audit Test Procedures
Application Controls Reviews, 445
IT Application Control Components
IT Application Controls, 426
IT Application Controls
Internal Audit Key Competencies, 425
Internal Auditor CBOK Requirements, 426
IT Application Control Components, 426
IT Databases, 429
IT Applications Development Reviews
Application Controls Reviews, 433
IT Auditing Background
Equity Funding, 382
IT Business Continuity Plans
BCP Risk and Business Impact Analysis, 517
Business Criticality Outage Impact Analysis, 518
Internal Audit Procedures, 515
IT Control Risks
Client-Server and Smaller IT Systems, 389
IT Controls
Control Activities, 27
COSO Internal Controls Framework, 42
IT Databases
IT Application Controls, 429
IT Disaster and Business Continuity Planning
Auditing Business Continuity Plans, 526
BCP Training, 523
Client-Server and Web-Based Applications, 507
Client-Server Continuity Planning Internal Audit Procedures, 513
Continuity Planning for Desktop and Laptop Applications, 513
Disaster Recovery Emergency Handling, 522
Emergency Response Plans, 512
IT Fraud Prevention Processes
Computer Forensics, 584
Fraud Detection and Prevention, 583
IT General Controls
Client-Server and Smaller IT Systems, 383
Internal Auditor CBOK Requirements, 381, 423
IT Internal Control Techniques. 381
ITIL Service Support and Delivery Infrastructure Best Practices, 405
IT Governance Focus Areas
CobiT, 91
IT Governance Institute (ITGI)
CobiT, 90
IT Infrastructure Controls
ITIL Configuration Management, 411
ITIL Service Support and Delivery Infrastructure Best Practices, 406
IT Internal Control Techniques.
IT General Controls, 381
IT Network Security Fundamentals
Cybersecurity Risks and Controls, 462
IT Passwords, 464
IT Security Threats, 462
IT System Firewalls, 468
Malicious Program Code Types, 466
Phishing and Other Identity Threats, 467
Security of Data, 463
Viruses and Malicious Program Code, 465
IT Password Logon Exchange Processes
IT Passwords, 465
IT Passwords
IT Network Security Fundamentals, 464
IT Password Logon Exchange Processes, 465
IT Processes
CobiT Cube Components, 95
IT Resources
CobiT Cube Components, 94
IT Risks and Controls
Internal Audit Attribute Standards, 189
IT Security Evaluation Framework
ISO 15408, 601
IT Security Requirements
ISO 27001 on IT Security, 674
IT Security Threats
IT Network Security Fundamentals, 462
IT Service-Level Agreement Contents
Service Level Agreements (SLAs), 416
IT System Firewalls
IT Network Security Fundamentals, 468

IT System Update Controls
Auditing IT General Controls, 392
IT Systems Privacy Concerns
Cybersecurity Risks and Controls, 469
Data Profiling Issues, 469
Internal Auditor General Understanding CBOK Needs, 470
Internet Privacy Threats, 470
ITIL Best Practices
ISO Standards, 665
ITIL Change Management
ITIL Framework, 413
ITIL Configuration Management
Internal Audit Steps, 412
IT Infrastructure Controls, 411
ITIL Framework
ITIL Change Management, 413
ITIL Service Delivery Availability Management, 421
ITIL Service Delivery Best Practices, 414
ITIL Service Delivery Capacity Management, 419
ITIL Service Delivery Continuity Management, 422
ITIL Service Delivery IT Financial Management, 418
ITIL Service Support Incident Management, 407
ITIL Service Support Problem Management, 409
ITIL Service Delivery Availability Management
ITIL Framework, 421
ITIL Service Delivery Best Practices
ITIL Framework, 414
ITIL Service Delivery Capacity Management
ITIL Framework, 419
ITIL Service Delivery Continuity Management
ITIL Framework, 422
ITIL Service Delivery IT Financial Management
Auditing IT Costs and Pricing, 419
ITIL Framework, 418
ITIL Service Delivery Service-Level Management
Service Level Agreements (SLAs), 415
ITIL Service Support and Delivery Infrastructure Best Practices
IT General Controls, 405
IT Infrastructure Controls, 406
ITIL Service Support Incident Management
ITIL Framework, 407
Service Level Agreements (SLAs), 407
ITIL Service Support Problem Management
ITIL Framework, 409

Judgmental Sampling
Audit Findings Problems, 204
Audit Sampling, 203

Key Example Company Characteristics
Global Computer Products Example Company, 240

Laptop Computers
Documenting Internal Audit Results, 340
Laptop-Based Internal Audit Systems
Document Backup, Security, and Continuity, 348
Large System IT General Controls Objectives
Auditing IT General Controls, 403
Launching a Consulting Assignment
Consulting Best Practices, 636
Lean Six Sigma
Lean Six Sigma Process Waste Example, 717
Quality Assurance Procedures, 716
Lean Six Sigma Process Waste Example
Lean Six Sigma, 717
Legacy System General Controls Reviews
Auditing IT General Controls, 400
Preliminary Reviews of IT General Controls, 400
Legal and Regulatory Compliance Requirements
Enterprise Risk Objectives, 143
Legal and Regulatory Compliance Risk Objectives
COSO ERM Framework, 143
Limitations/Problems with IIARF CBOK Survey
IIARF CBOK Evaluation Results, 15
Limitations on External Auditor Services
SOx Section 201, 60
SOx Title II: Auditor Independence, 60
Loss Event Data Tracking
Risk Identification Processes, 134

Mainframe and Legacy Systems
Auditing IT General Controls, 394
Malicious Program Code Types
IT Network Security Fundamentals, 466

Management Agreements to IIARF CBOK Survey Results
IIA Standards Compliance, 16
Management's Philosophy and Operating Style
Control Environment, 36
Management's Assessment of Internal Controls
SOx Title IV: Enhanced Financial Disclosures, 69
Mapping Internal Control Frameworks
COSO and CobiT Relationships, 109
Mesopotamian Civilizations
Foundations of Internal Auditing, 3
Methods of Communication
Communications and Information, 32
Microsoft Corporate Internal Audit CAA Approach
Technology Enabled Continuous Auditing (TECA) System, 649
Microsoft Corporation's 2007 Audit Committee Charter
Audit Committee Charters, 536
Misappropriation of Assets
Fraud Risk Factors, 579
Mission Statements
Ethics and Whistleblower Programs, 551
Modern Internal Auditing
Book Objective, 3
Definition, 3
IIA Definition, 4
Monetary Unit Sampling
Audit Sampling, 225
Evaluating Monetary Unit Sample Results, 228
Monetary Unit Sampling Selection Example, 226
Monetary Unit Sampling Selection Example
Monetary Unit Sampling, 226
Monitoring
Communications from External Parties, 47
COSO Internal Controls Framework, 32
COSO Internal Controls Framework, 46
Internal Control Evaluations, 34
Reporting Internal Control Deficiencies, 35
Moto of The Institute of Internal Auditors
Progress through Sharing, 11
Multistage Sampling
Audit Sampling Approaches, 232

National Commission on Fraudulent Financial Reporting
Treadway Committee, 31
Treadway Committee, 31
Navigating the CobiT Framework
CobiT, 97
Negative Assurance
Internal Control Definitions, 29
New Internal Audit Standards
International Standards for the Professional Practice of Internal Auditing, 187
Normal Distributions
Statistical Sampling Concepts, 209
NYSE Model Audit Committee Charter
Audit Committee Organization and Charters, 535

Objectives and Obstacles of Reimplementation Auditing
Auditing Applications under Development, 452
Objectives of IIARF CBOK
IIARF CBOK Survey, 14
Objectives of this Book
Practice of Modern Internal Auditing, 9
Object-Oriented Programming Language Concepts
Computer Programming Languages, 432
Off Balance-sheet Transactions
SOx Title IV: Enhanced Financial Disclosures, 68
Online Analytical Processing (OLAP)
Continuous Monitoring Processes, 658
Operating Systems Software
Characteristics of Larger IT Systems, 398
Operations Risk Management Objectives
COSO ERM Framework, 142
Oral or Informal Audit Reports
Audit Report Formats, 365
Organization Project Management (OPM3)
Project Management, 306
Organizational Process Maturity Model
Project Management Processes, 315
Organizational Structure
Control Environment, 36
Organizing Section 404 Compliance Review Projects
Section 404 Compliance Reviews, 79
Organizing and Conducting a CSA Process
Internal Auditor CBOK Requirements, 262

Organizing and Planning Internal Audits
Audit Plan Project Schedule Example, 156
International Standards for the Professional Practice of Internal Auditing, 154
Origins – First Membership Chapter
IIA, 5
Institute of Internal Auditors, 5

Pareto Chart Example
Quality Audit Tools and Techniques, 683
Payment System Continuous Audit Monitor
Continuous Monitoring Processes, 646
PCAOB Accounting Standards Authority
Financial Accounting Standards Board (FASB), 59
SOx Title I: Public Company Accounting Oversight Board, 59
PCAOB Administration and Public Accounting Firm Registration
SOx Title I: Public Company Accounting Oversight Board, 56
PCAOB Auditing, Quality Control, and Independence Standards
SOx Title I: Public Company Accounting Oversight Board, 56
PCAOB Standard AS 3
Workpaper Retention Rules, 57
PCAOB Standard AS 5
Sarbanes-Oxley Act Key Provisions, 57
PCI-DSS Requirements
Cybersecurity and Privacy Controls, 478
PDCA Continuous Improvement Cycle
Performing ASQ Quality Audits, 686
Pension Fund Blackout Periods
SOx Title III: Corporate Responsibility, 67
Performing a Benchmarking Study
Internal Audit Roles, 265
Performing an Individual Internal Audit
Audit Assessment and Evaluation Techniques, 200
Audit Evidence, 199
Internal Audit Process Steps, 181
Performing Applications Controls Reviews
Auditing Applications under Development, 451
Automated Purchasing System Compliance Tests, 447
Developing Application Control Objectives, 442
Internal Audit Key Competencies, 437
Testing Audit Internal Control Objectives, 444
Performing ASQ Quality Audits
PDCA Continuous Improvement Cycle, 686
Quality Audit Process Steps, 687
Quality Audit Tools and Techniques, 685
Performing Effective Internal Audits
Internal Audit Preparatory Activities, 155
Internal Auditor CBOK Requirements, 153
Performing Effective QA Reviews
Internal Auditor CBOK Requirements, 705
Performing Facilitated CSA Reviews
CSA Facilitated Sessions, 258
Internal Audit Roles, 257
Performing the Internal Audits
Internal Audit Fieldwork Procedures, 173
Internal Auditor CBOK Requirements, 172
Workpaper Review "Point Sheets", 174
Permanent files
Workpaper Document Organization, 341
Phishing and Other Identity Threats
IT Network Security Fundamentals, 467
Planning and Performing Internal Audits
Developing Appropriate Internal Audit Procedures, 324
Internal Auditor CBOK Requirements, 321
Walk-through Exercises, 324
Planning Internal Audit Activities
Audit Focal Points, 239
PMI Standard for Program Management
Program and Portfolio Management, 311
PMI's PMBOK
Definition of a CBOK, 12
PMP (Project Management Professional)
Project Management, 306
Practice of Internal Auditing
Fraud Detection and Prevention, 585
International Standards for the Professional Practice of Internal Auditing, 580
Practice of Modern Internal Auditing
Objectives of this Book, 9
Preliminary Audit Findings
Audit Findings, 177
Preliminary Findings Point Sheets
Audit Fieldwork, 328
Preliminary Reviews of IT General Controls
Legacy System General Controls Reviews, 400
Preliminary Surveys
Internal Audit Planning, 159
Internal Audit Self-Assessments, 159

Pro forma Financial Reports
SOx Title IV: Enhanced Financial Disclosures, 68
Probability Estimates
Risk Assessments, 119
Procedure Oriented Audit Programs
Audit Programs, 171
Process Model Example
Documenting Internal Audit Results, 331
Process Modeling and Workpapers
Documenting Internal Audit Results, 329
Process Modeling for Internal Auditors
Input/Output Process Flowchart, 334
Internal Auditor CBOK Requirements, 329
Work-Flow Description Process Flowcharts, 334
Process Modeling Hierarchy
Documenting Internal Audit Results, 333
Professional Certifications
ASQ Internal Audit Certifications, 625
Certified Fraud Examiner (CFE) Certification, 623
Certified Information Security Manager® (CISM) Certification, 622
Certified Information Systems Auditor (CISA) Requirements, 619
Certified Information Systems Security Professional (CISSP) Certification, 624
Certified Internal Auditor Responsibilities and Requirements, 606
CIA Responsibilities and Requirements, 606
Program and Portfolio Management
PMI Standard for Program Management, 311
Progress through Sharing
Moto of The Institute of Internal Auditors, 11
Project Management
Developing a Project Management Plan, 310
Effective Internal Audit Plans, 318
Internal Audit Key Competencies, 310
Organization Project Management (OPM3), 306
PMP (Project Management Professional), 306
Project Management Book of Knowledge (PMBOK), 306
Project Management Best Practices
Internal Audit Key Competencies, 319
Project Management Book of Knowledge (PMBOK)
Project Management, 306
Project Management Knowledge Areas, 308
Project Management Knowledge Areas
Project Management Book of Knowledge (PMBOK), 308
Project Management Processes
Internal Audit Key Competencies, 305
Organizational Process Maturity Model, 315
Public Accounting Firm Prohibitions
Financial Information Systems Design, 61
SOx Title II: Auditor Independence, 61
Public Accounting's Role in Fraud Detection
AICPA SAS No. 99, 577
Public Company Accounting Oversight Board (PCAOB)
Sarbanes-Oxley Act (SOx), 53
Purchased Software Internal Controls Audit Checklist
Application Controls Reviews, 435

Quality Assurance and Improvement Programs
Internal Audit Attribute Standards, 190
International Standards for the Professional Practice of Internal Auditing, 190
Quality Assurance Auditing (ASQ) Standards
Internal Audit Key Competancies, 679
Quality Auditor Duties and Responsibilities, 680
Quality Assurance Procedures
Lean Six Sigma, 716
Six Sigma Background and Concepts, 708
Quality Assurance Review of Internal Audit Review Steps
Internal Audit Function Internal Quality Assurance Reviews, 699
Quality Assurance Reviews
Internal Audit Function, 688
Quality Audit Approaches
Classifications of Quality Audits, 682
Quality Audit Process Steps
IIA Internal Auditors, 687
Performing ASQ Quality Audits, 687
Quality Audit Tools and Techniques
Pareto Chart Example, 683
Performing ASQ Quality Audits, 685

Quality Auditor Duties and Responsibilities
ASQ Quality Audit Division (QAD), 680
ISO 27001 Internal Audit Standards, 684
Quality Assurance Auditing (ASQ) Standards, 680
Quality Management System Process
ISO 9001 on Quality Management Systems, 669
Quality Management Techniques
IIARF CBOK Evaluation Results, 16
Quality of Information
Communications and Information, 29
COSO Internal Controls Framework, 44
Quality Review Engagement Letters
Internal Audit Function Internal Quality Assurance Reviews, 696
Quality-Assurance Auditee Review Questions
Internal Audit Function Internal Quality Assurance Reviews, 703
Quality-Assurance Auditing
Future Directions for Quality-Assurance Auditing, 704
Quality-Assurance Review Approaches
Internal Audit Function Internal Quality Assurance Reviews, 695
Quality-Assurance Review of Internal Audit
Internal Audit Procedures, 691
Quantitative Risk Analysis
Risk Management Fundamentals, 121
Questionnaire-Format Audit Reports
Audit Report Formats, 366

RACI Chart Responsibilities
CobiT Objectives, 99
Radio Frequency Identification
Internet Privacy Threats, 470
Random Number Sample Selections
Statistical Sampling Plans, 211
Reasons for Committing Fraud
Definition of a Fraud, 576
Red Book
International Standards for the Professional Practice of Internal Auditing, 183
Red Flags Indicating Potential Financial Fraud
Fraud Detection and Prevention, 574
Reimplementation Internal Audit Reviews
Application Controls Reviews, 433
Reimplementation Review Application Testing Checklist
Reimplementation Review Procedures, 458
Reimplementation Review Objectives
Auditing Applications under Development, 453
Reimplementation Review Problems
Auditing Applications under Development, 454
Reimplementation Review Procedures
Auditing Applications under Development, 455
Reimplementation Review Application Testing Checklist, 458
Reimplementation Review Requirements Definition Checklist, 456
Reimplementation Review Requirements Definition Checklist
Reimplementation Review Procedures, 456
Replicated Sampling
Audit Sampling Approaches, 232
Report Generators Languages
Types of CAATTs, 489
Reporting Internal Audit Results
Audit Exit or Closing Conferences, 370
Effective Internal Audit Communications, 374
Internal Audit Reports, 351
Reporting Internal Control Deficiencies
COSO Internal Controls Framework, 48
Monitoring, 35
Reporting Risk Management Objectives
COSO ERM Framework, 143
Residual Risk
Risk Assessment, 134
Reviews of IT and Cybersecurity Controls
Auditing IT Security and Privacy, 472
Risk Acceptance
Risk Response Strategies, 136
Risk Appetite
COSO ERM Internal Environment, 128
Risk Management Fundamentals, 125
Risk Appetite Map
Risk Objective Setting, 130
Risk Assessment
COSO Internal Controls Framework, 39
Inherent Risk, 134
Residual Risk, 134
Risk Assessment as a Three-Step Process, 39
COSO Internal Controls Framework, 23

Risk Assessment Analysis Map
Risk Assessments, 119
Risk Assessment as a Three-Step Process
Risk Assessment, 39
Risk Assessment Process
COSO Internal Controls Framework, 23
Risk Assessment Processes
Control Activities, 26
External Factor Risks, 23
Internal Factor Risks, 23
Specific Activity-Level Risks, 24
Risk Assessments
COSO Enterprise Risk Management (COSO ERM), 113
Probability Estimates, 119
Risk Assessment Analysis Map, 119
Risk Management Fundamentals, 118
Risk Avoidance
Risk Response Strategies, 136
Risk Event Identification
COSO ERM Internal Environment, 132
Risk Events
Union Carbide in Bhopal, India, 121
Risk Identification
Enterprise Risks, 117
Enterprise-Wide Strategic Risks, 117
Risk Management Fundamentals, 115
Risk Identification Processes
Loss Event Data Tracking, 134
Risk Independencies
Risk Management Fundamentals, 120
Risk Likelihood and Impact Mapping
Risk Response Strategies, 135
Risk Management
AS 5 Key Concepts, 113
Internal Audit Performance Standards, 192
Risk Management Fundamentals
COSO ERM, 114
Effective Risk Management Processes, 115
Quantitative Risk Analysis, 121
Risk Appetite, 125
Risk Assessments, 118
Risk Identification, 115
Risk Independencies, 120
Risk Ranking Expected Costs, 123
Risk Scoring Schedules, 120
Risk Management Philosophy
COSO ERM Framework, 127
COSO ERM Internal Environment, 127
Risk Objective Setting
COSO ERM Internal Environment, 130
Risk Appetite Map, 130
Risk Ranking Expected Costs
Risk Management Fundamentals, 123
Risk Response Strategies
Risk Acceptance, 136
Risk Avoidance, 136
Risk Likelihood and Impact Mapping, 135
Risk Scoring Schedules
Risk Management Fundamentals, 120
Root Cause Analysis
Service Support Problem Management Processes, 410

Sample Organization Chart
Global Computer Products Example Company, 242
Sample Size Recommendations
Section 404 Compliance Reviews, 83
Sampling Advantages and Limitations
Attributes Sampling, 224
Sarbanes-Oxley Act (SOx)
Auditing Business Continuity Planning Processes, 508
Sarbanes-Oxley Act (SOx) Requirements, 510
Cox Title XI: Corporate Fraud Accountability, 74
Public Company Accounting Oversight Board (PCAOB), 53
Sarbanes-Oxley Act Key Provisions, 55
Section 404 Compliance Reviews, 76
Section 404 Internal Controls Assessments, 75
SOx Background, 53
SOx Important Aspects, 54
SOx Title II: Auditor Independence, 60
SOx Title III: Corporate Responsibility, 62
SOx Title IV: Enhanced Financial Disclosures, 68
SOx Title V: Analyst Conflicts of Interest, 72
Sarbanes-Oxley Act (SOx) Requirements
Sarbanes-Oxley Act (SOx), 510
Sarbanes-Oxley Act Key Provisions
Auditing Standard No. 5 (AS 5), 57
PCAOB Standard AS 5, 57
Sarbanes-Oxley Act (SOx), 55
Workpaper Retention Rules, 57
SAS No. 55
Financial Auditing Standards, 30
Internal Control Structure in a Financial Statement Audit, 30
Internal Control Definitions, 30

SEC Audit Committee Rules
  Audit Committee Financial Expert Rules, 537
  Audit Committee Governance, 533
Section 302 Corporate Responsibility for Financial Reports
  SOx Title III: Corporate Responsibility, 63
Section 404 Compliance Reviews
  Basic Accounting Cycles, 76
  Internal Audit Roles, 84
  Internal Audit's Role, 78
  Organizing Section 404 Compliance Review Projects, 79
  Recommended Sample Sizes, 83
  Sarbanes-Oxley Act (SOx), 76
  Selecting Key Processes for Review, 80
  Transaction Flow Documentation, 81
Section 404 Internal Controls Assessments
  Sarbanes-Oxley Act (SOx), 75
Section 404 Reviews under AS, 5
  SOx Section 404 Internal Controls Assessments, 75
Securities Exchange Act of 1934
  Controls Standards Background, 25
Security and Control for Auditor Computers
  Security and Privacy in the Internal Audit Department, 474
Security and Privacy in the Internal Audit Department
  Audit Reports and Privacy, 477
  Cybersecurity Risks and Controls, 474
  Security and Control for Auditor Computers, 474
  Workpaper Security, 475
  Workpaper Security Best Practices, 476
Security of Data
  IT Network Security Fundamentals, 463
Selecting and Printing Audit Samples
  CAATT Procedures, 487
Selecting Appropriate CAATT Processes
  Basic Understandings of the General Use of CAATTs, 501
Selecting Key Processes for Review
  Section 404 Compliance Reviews, 80
Service Level Agreements (SLAs)
  IT Service-Level Agreement Contents, 416
  ITIL Service Delivery Service-Level Management, 415
  ITIL Service Support Incident Management, 407
Service Support Problem Management Processes
  Root Cause Analysis, 410
Service to Management
  Internal Audit Roles, 8
Service-Level Agreements (SLAs)
  Business Continuity Planning, 523
Significant Internal Audit Findings
  Audit Committee Review and Action, 545
Signing Officer Certification of Financial Reports
  SOx Title III: Corporate Responsibility, 63
Six Sigma Background and Concepts
  Baldridge National Quality Award, 708
  Black Belt Body of Knowledge, 712
  Implementing Six Sigma, 709
  Quality Assurance Procedures, 708
  Six Sigma Design-Measure-Analyze-Improve-Control (DMAIC) Model, 708
  Six Sigma SIPOC Chart, 715
Six Sigma Deployment and Process Guide
  Implementing Six Sigma, 710
Six Sigma Design-Measure-Analyze-Improve-Control (DMAIC) Model
  DMAIC Procedures for a Six Sigma Project, 715
  Six Sigma Background and Concepts, 708
Six Sigma Leadership Roles and Responsibilities
  Implementing Six Sigma, 711
Six Sigma Principles
  Internal Auditor CBOK Requirements, 721
Six Sigma SIPOC Chart
  Six Sigma Background and Concepts, 715
Slush Funds
  Foreign Corrupt Practices Act of 1977 (FCPA), 27
Smaller Business IT Systems
  General Control Objectives, 393
SOx Audit Committee Whistleblower Rules
  Whistleblower and Hotline Functions, 563
SOx Background
  Sarbanes-Oxley Act (SOx), 53
SOx Closing Requirements
  Continuous Close Processes, 659
SOx Important Aspects
  Sarbanes-Oxley Act (SOx), 54
  Whistleblower Programs, 54
SOx Requirements
  Audit Committee Formal Whistleblower Programs, 547
SOx Section 201
  Limitations on External Auditor Services, 60

SOx Section 302 Officer Certifications
SOx Title III: Corporate Responsibility, 65
SOx Section 404 Internal Controls Assessments
CobiT, 108
CobiT, 90
COSO Internal Controls Framework, 76
Section 404 Reviews under AS 5, 75
SOx Title IV: Enhanced Financial Disclosures, 69
SOx Section 404 Internal Controls Tests
Attributes Sampling, 216
SOx Section 404 Requirements
COSO ERM Risk Event Identification, 138
SOx Title I: Public Company Accounting Oversight Board
Audit Quality Control Standards, 58
Concurring Partner Approvals, 58
Inspections, Investigations, and Disciplinary Procedures, 59
Internal Control Testing Scope, 58
PCAOB Accounting Standards Authority, 59
PCAOB Administration and Public Accounting Firm Registration, 56
PCAOB Auditing, Quality Control, and Independence Standards, 56
SOx Title II: Auditor Independence
Audit Committee Preapproval of Services, 61
External Audit Conflicts of Interest, 62
Internal Auditor Outsourcing, 60
Limitations on External Auditor Services, 60
Public Accounting Firm Prohibitions, 61
Sarbanes-Oxley Act (SOx), 60
SOx Title III: Corporate Responsibility
Pension Fund Blackout Periods, 67
Sarbanes-Oxley Act (SOx), 62
Section 302 Corporate Responsibility for Financial Reports, 63
Signing Officer Certification of Financial Reports, 63
SOx Section 302 Officer Certifications, 65
SOx Title IV: Enhanced Financial Disclosures
Enterprise Codes of Conduct, 71
Financial Officer Codes of Conduct, 70
Management's Assessment of Internal Controls, 69
Off Balance-Sheet Transactions, 68
Pro forma Financial Reports, 68
Sarbanes-Oxley Act (SOx), 68
SOx Section 404 Internal Controls Assessments, 69
SOx Title V: Analyst Conflicts of Interest
Sarbanes-Oxley Act (SOx), 72
SOx Title XI: Corporate Fraud Accountability
Sarbanes-Oxley Act (SOx), 74
SOx Whistleblower Call Center Guidelines
Ethics and Whistleblower Programs, 565
SOx Whistleblower Rules
Internal Audit Roles and Responsibilities, 564
Specialized Audit Test and Analysis Software
Computer-Aided Systems Engineering (CASE) Software Tools, 496
Types of CAATTs, 496
Specific Activity-Level Risks
Risk Assessment Processes, 24
Standard Deviations
Statistical Sampling Concepts, 207
Standards for the Professional Practice of Internal Auditing
CBOK Objectives, 18
Controls Definition, 25
Statistical Sampling Concepts
Audit Sampling, 205
Histograms, 207
Normal Distributions, 209
Standard Deviations, 207
Statistical Sampling Plans
Audit Sampling, 210
Cluster Selection Sampling, 213
Interval Selection Sampling, 211
Random Number Sample Selections, 211
Stratified Selection Sampling, 212
Stratified Variables Sampling, 229
Strategic and Integrated Systems
Communications and Information, 29
COSO Internal Controls Framework, 44
Stratified Selection Sampling
Statistical Sampling Plans, 212
Stratified Variables Sampling
Statistical Sampling Plans, 229
Summarizing Ethics Survey Results
Ethics Environment Attitude Surveys, 556
Surprise Audits
Internal Audit Planning, 162

Switchable Hot Site Facilities
BCP Contingency Strategies, 519
Systems Development Life Cycle (SDLC) Procedures
CobiT Domain Areas, 95
Systems Development Methodology (SDM) Processes
Application Controls Reviews, 438

Technical Security Services and Mechanisms
HIPAA: Healthcare Related Rules, 594
Technology Enabled Continuous Auditing (TECA) System
Microsoft Corporate Internal Audit CAA Approach, 649
Temptations that Encourage Improper Accounting
Integrity and Ethical Values, 35
Test Deck Approaches
Tracing User-Initiated Transactions, 494
Types of CAATTs, 492
Testing and Analysis Skills
Internal Auditor Communication Skills, 296
Testing Audit Internal Control Objectives
Performing Applications Controls Reviews, 444
Testing Calculations and Making Computations
CAATT Procedures, 486
The Institute of Internal Auditors (IIA)
Code of Ethics, 197
Tick Marks
Workpaper Document Organization, 346
Tone at the Top
Control Environment, 34
Tracing User-Initiated Transactions
Test Deck Approaches, 494
Traditional Hot Sites
BCP Contingency Strategies, 519
Transaction Flow Documentation
Section 404 Compliance Reviews, 81
Treadway Commission
Internal Control Definitions, 28
Treadway Committee
National Commission on Fraudulent Financial Reporting, 31
Treadway Committee Report
COSO Internal Control Framework, 31
Internal Control Definitions, 31

U.S. Federal Whistleblower Rules
Whistleblower and Hotline Functions, 563
U.S. Securities and Exchange Commission (SEC) Rules
International Accounting and Auditing Standards, 724
International Financial Reporting Standards (IFRS), 723
Understanding and Recognizing Fraud
Fraud Detection and Prevention, 572
Understanding Current IIA Standards
Internal Auditor CBOK Requirements, 183
Understanding HIPAA or GLBA Rules
Internal Auditor CBOK Requirements, 601
Understanding of BCP Requirements
Internal Auditor CBOK Requirements, 527
Understanding of Six Sigma Processes
Internal Auditor CBOK Requirements, 709
Unethical, Illegal, or Otherwise Improper Activities
COSO Internal Controls Framework, 45
Union Carbide in Bhopal, India
Risk Events, 121

Variables Sampling
Audit Sampling Approaches, 215
Victor Z. Brink
History of Internal Auditing, 5
Internal Auditing History, 5
Viruses and Malicious Program Code
IT Network Security Fundamentals, 465

Walk-through Exercises
Planning and Performing Internal Audits, 324
Whistleblower and Hotline Functions
Ethics and Whistleblower Programs, 562
SOx Audit Committee Whistleblower Rules, 563
U.S. Federal Whistleblower Rules, 563
Whistleblower Programs
Communications and Information, 45
SOx Important Aspects, 54
Whistleblower Responsibilities
Audit Committee Roles and Responsibilities, 546
Work-Flow Description Process Flowcharts
Process Modeling for Internal Auditors, 334
Workpaper Auditor Tick Marks
Workpaper Document Organization, 346

Workpaper Cross-Referencing
Workpaper Document Organization, 346
Workpaper Document Organization
Administrative files, 341
Audit Procedures Files, 342
Documenting Internal Audit Results, 340
Internal Audit Document Records Management, 348
Internal Audit Documentation Requirements, 348
Permanent Files, 341
Tick Marks, 346
Workpaper Auditor Tick Marks, 346
Workpaper Cross-Referencing, 346
Workpaper Indexing and Cross-Referencing, 345
Workpaper Preparation Techniques, 345
Workpaper Supervisor Point Sheets, 344
Workpaper Indexing and Cross-Referencing
Workpaper Document Organization, 345
Workpaper Objectives
Documenting Internal Audit Results, 336
Workpaper Permanent Files
Documenting the Internal Audit Field Surveys, 166
Workpaper Preparation Techniques
Workpaper Document Organization, 345
Workpaper Review Processes, 347
Workpaper Retention Rules
PCAOB Standard AS 3, 57
Sarbanes-Oxley Act Key Provisions, 57
Workpaper Review "Point Sheets"
Performing the Internal Audits, 174
Workpaper Review Processes
CAATT Document Repositories, 349
Chief Audit Executive (CAE) Overall Workpaper Responsibility, 347
Document Backup, Security, and Continuity, 348
Document Standards and Review Processes, 348
Workpaper Preparation Techniques, 347
Workpaper Security
Security and Privacy in the Internal Audit Department, 475
Workpaper Security Best Practices
Security and Privacy in the Internal Audit Department, 476
Workpaper Standards
Audit Bulk Files, 344
International Standards for the Professional Practice of Internal Auditing, 338
Workpaper Supervisor Point Sheets
Workpaper Document Organization, 344

XBRL Defined
XBRL: Internet-Based Extensible Business Reporting Language, 652
XBRL: Internet-Based Extensible Business Reporting Language
Financial and Business Reporting Tools, 651
Implementing XBRL, 653
XBRL Defined, 652