# Contents

- **Preface**
  - xxv
- **About the Author**
  - xxv

## PART ONE
**FOUNDATIONS OF MODERN INTERNAL AUDITING**

### CHAPTER 1
Foundations of Internal Auditing

1.1 Internal Auditing History and Background

1.2 Organization of This Book

Note

### CHAPTER 2
Internal Audit’s Common Body of Knowledge

2.1 What Is a CBOK?: Experiences from Other Professions

2.2 Institute of Internal Auditor’s Research Foundation CBOK

2.3 What Does an Internal Auditor Need to Know?

2.4 Modern Internal Auditing’s CBOK Going Forward

Notes

## PART TWO
**IMPORTANCE OF INTERNAL CONTROLS**

### CHAPTER 3
Internal Control Framework: The COSO Standard

3.1 Importance of Effective Internal Controls

3.2 Internal Controls Standards: Background

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

  (b) FCPA Aftermath: What Happened?

3.3 Events Leading to the Treadway Commission

  (a) Earlier AICPA Standards: SAS No. 55

  (b) Treadway Committee Report

3.4 COSO Internal Control Framework

  (a) Control Environment

  (b) Risk Assessment

  (c) Control Activities

  (d) Communications and Information

  (e) Monitoring

Notes
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
(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 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
|
|---|
|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 Notes | 318|
|**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|
PART FIVE

IMPACT OF INFORMATION TECHNOLOGY ON INTERNAL AUDITING

CHAPTER 18

IT General Controls and ITIL Best Practices

18.1 Importance of IT General Controls
18.2 Client-Server and Smaller Systems' General IT Controls
   (a) General Controls for Small Business Systems
   (b) Smaller Systems' IT Operations Internal Controls
   (c) Auditing IT General Controls for Smaller IT Systems
18.3 Components and Controls of Mainframe and Legacy Systems
   (a) Characteristics of Larger IT Systems
   (b) Classic Mainframe or Legacy Computer Systems
   (c) Operating Systems Software
18.4 Legacy System General Controls Reviews
18.5 ITIL Service Support and Delivery Infrastructure Best Practices
   (a) ITIL Service Support Incident Management
   (b) Service Support Problem Management
18.6 Service Delivery Best Practices
   (a) Service Delivery Service-Level Management
   (b) Service Delivery Financial Management for IT Services
   (c) Service Delivery Capacity Management
   (d) Service Delivery Availability Management
   (e) Service Delivery Continuity Management
18.7 Auditing IT Infrastructure Management
18.8 Internal Auditor CBOK Needs for IT General Controls

CHAPTER 19

Reviewing and Assessing IT Application Controls

19.1 IT Application Control Components
   (a) Application Input Components
   (b) Application Programs
   (c) IT Application Output Components
## Contents

### 19.2 Selecting Applications for Internal Audit Reviews

### 19.3 Preliminary Steps to Performing Applications Controls Reviews
- (a) Conducting an Application Walk-Through
- (b) Developing Application Control Objectives

### 19.4 Completing the IT Application’s Controls Audit
- (a) Clarifying and Testing Audit Internal Control Objectives
- (b) Completing the Application Controls Review

### 19.5 Application Review Example: Client-Server Budgeting System
- (a) Reviewing Capital Budgeting System Documentation
- (b) Identifying Capital Budgeting Application Key Controls
- (c) Performing Application Tests of Compliance

### 19.6 Auditing Applications under Development
- (a) Objectives and Obstacles of Preimplementation Auditing
- (b) Preimplementation Review Objectives
- (c) Preimplementation Review Problems
- (d) Preimplementation Review Procedures

### 19.7 Importance of Reviewing IT Application Controls

### Notes

---

### CHAPTER 20 Cybersecurity and Privacy Controls

#### 20.1 IT Network Security Fundamentals
- (a) Security of Data
- (b) Importance of IT Passwords
- (c) Viruses and Malicious Program Code
- (d) Phishing and Other Identity Threats
- (e) IT System Firewalls
- (f) Other Computer Security Issues

#### 20.2 IT Systems Privacy Concerns
- (a) Data Profiling Privacy Issues
- (b) Online Privacy and E-Commerce Issues
- (c) Radio Frequency Identification
- (d) Absence of U.S. Federal Privacy Protection Laws

#### 20.3 Auditing IT Security and Privacy

#### 20.4 Security and Privacy in the Internal Audit Department
- (a) Security and Control for Auditor Computers
- (b) Workpaper Security
- (c) Audit Reports and Privacy
- (d) Internal Audit Security and Privacy Standards and Training

#### 20.5 PCI-DSS Fundamentals

#### 20.6 Internal Audit’s Privacy and Cybersecurity Roles

### Notes
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

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

PART EIGHT  INTERNAL AUDITING PROFESSIONAL CONVERGENCE  
CBOK REQUIREMENTS  

CHAPTER 30  ISO 27001, ISO 9000, and Other International Standards  
30.1 Importance of ISO Standards in Today's Global World  
30.2 ISO Standards Overview  
(a) ISO 9001 Quality Management Systems and Sarbanes-Oxley  
(b) IT Security Standards: ISO 17799 and 27001  
(c) IT Security Technique Requirements: ISO 27001  
(d) Service Quality Management: ISO 20000  
30.3 ISO 19011 Quality Management Systems Auditing  
30.4 ISO Standards and Internal Auditors  
Notes  

CHAPTER 31  Quality Assurance Auditing and ASQ Standards  
31.1 Duties and Responsibilities of Quality Auditors  
31.2 Role of the Quality Auditor  
31.3 Performing ASQ Quality Audits  
31.4 Quality Auditors and the IIA Internal Auditor  
31.5 Quality Assurance Reviews of the Internal Audit Function  
(a) Benefits of an Internal Audit Quality-Assurance Review  
(b) Elements of an Internal Audit Quality-Assurance Review  
(c) Who Performs the Quality-Assurance Review?  
31.6 Launching the Internal Audit Quality-Assurance Review  
(a) Quality-Assurance Review Approaches
(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