Contents

Preface xvii

PART ONE: FOUNDATIONS OF MODERN INTERNAL AUDITING

Chapter 1: Significance of Internal Auditing in Enterprises Today: An Update 3

1.1 Internal Auditing History and Background 5
1.2 Mission of Internal Auditing 9
1.3 Organization of this Book 9
Note 10

Chapter 2: An Internal Audit Common Body of Knowledge 11

2.1 What Is a CBOK? Experiences from Other Professions 12
2.2 What Does an Internal Auditor Need to Know? 14
2.3 An Internal Auditing CBOK 14
2.4 Another Attempt: The IIA Research Foundation's CBOK 20
2.5 Essential Internal Audit Knowledge Areas 25
Notes 25

PART TWO: IMPORTANCE OF INTERNAL CONTROLS

Chapter 3: The COSO Internal Control Framework 29

3.1 Understanding Internal Controls 30
3.2 Revised COSO Framework Business and Operating Environment Changes 33
3.3 The Revised COSO Internal Control Framework 35
3.4 COSO Internal Control Principles 37
3.5 COSO Internal Control Components: The Control Environment 38
3.6 COSO Internal Control Components: Risk Assessment 40
3.7 COSO Internal Control Components: Internal Control Activities 45
3.8 COSO Internal Control Components: Information and Communication 49
3.9 COSO Internal Control Components: Monitoring Activities 53
3.10 The COSO Framework’s Other Dimensions 57
## Chapter 4: The 17 COSO Internal Control Principles

<table>
<thead>
<tr>
<th>Principle</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 COSO Internal Control Framework Principles</td>
<td>59</td>
</tr>
<tr>
<td>4.2 Control Environment Principle 1: Integrity and Ethical Values</td>
<td>60</td>
</tr>
<tr>
<td>4.3 Control Environment Principle 2: Role of the Board of Directors</td>
<td>64</td>
</tr>
<tr>
<td>4.4 Control Environment Principle 3: Authority and Responsibility Needs</td>
<td>65</td>
</tr>
<tr>
<td>4.5 Control Environment Principle 4: Commitment to a Competent Workforce</td>
<td>66</td>
</tr>
<tr>
<td>4.6 Control Environment Principle 5: Holding People Accountable</td>
<td>67</td>
</tr>
<tr>
<td>4.7 Risk Assessment Principle 6: Specifying Appropriate Objectives</td>
<td>68</td>
</tr>
<tr>
<td>4.8 Risk Assessment Principle 7: Identifying and Analyzing Risks</td>
<td>68</td>
</tr>
<tr>
<td>4.9 Risk Assessment Principle 8: Evaluating Fraud Risks</td>
<td>69</td>
</tr>
<tr>
<td>4.10 Risk Assessment Principle 9: Identifying Changes Affecting Internal Controls</td>
<td>71</td>
</tr>
<tr>
<td>4.11 Control Activities Principle 10: Selecting Control Activities That Mitigate Risks</td>
<td>72</td>
</tr>
<tr>
<td>4.12 Control Activities Principle 11: Selecting and Developing Technology Controls</td>
<td>73</td>
</tr>
<tr>
<td>4.13 Control Activities Principle 12: Policies and Procedures</td>
<td>74</td>
</tr>
<tr>
<td>4.14 Information and Communication Principle 13: Using Relevant, Quality Information</td>
<td>75</td>
</tr>
<tr>
<td>4.15 Information and Communication Principle 14: Internal Communications</td>
<td>78</td>
</tr>
<tr>
<td>4.16 Information and Communication Principle 15: External Communications</td>
<td>81</td>
</tr>
<tr>
<td>4.17 Monitoring Principle 16: Internal Control Evaluations</td>
<td>82</td>
</tr>
<tr>
<td>4.18 Monitoring Principle 17: Communicating Internal Control Deficiencies</td>
<td>83</td>
</tr>
</tbody>
</table>

## Chapter 5: Sarbanes-Oxley (SOx) and Beyond

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Key Sarbanes-Oxley Act (SOx) Elements</td>
<td>86</td>
</tr>
<tr>
<td>5.2 Performing Section 404 Reviews under AS5</td>
<td>107</td>
</tr>
<tr>
<td>5.3 AS5 Rules and Internal Audit</td>
<td>118</td>
</tr>
<tr>
<td>5.4 Impact of the Sarbanes-Oxley Act</td>
<td>120</td>
</tr>
<tr>
<td>Notes</td>
<td>121</td>
</tr>
</tbody>
</table>

## Chapter 6: COBIT and Other ISACA Guidance

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 Introduction to COBIT</td>
<td>124</td>
</tr>
<tr>
<td>6.2 COBIT Framework</td>
<td>126</td>
</tr>
<tr>
<td>6.3 Principle 1: Meeting Stakeholder Needs</td>
<td>128</td>
</tr>
<tr>
<td>6.4 Principle 2: Covering the Enterprise End to End</td>
<td>129</td>
</tr>
<tr>
<td>6.5 Principle 3: A Single Integrated Framework</td>
<td>131</td>
</tr>
<tr>
<td>6.6 Principle 4: Enabling a Holistic Approach</td>
<td>132</td>
</tr>
<tr>
<td>6.7 Principle 5: Separating Governance from Management</td>
<td>134</td>
</tr>
<tr>
<td>6.8 Using COBIT to Assess Internal Controls</td>
<td>135</td>
</tr>
<tr>
<td>6.9 Mapping COBIT to COSO Internal Controls</td>
<td>139</td>
</tr>
<tr>
<td>Notes</td>
<td>139</td>
</tr>
</tbody>
</table>
# Chapter 11: Continuous Auditing and Computer-Assisted Audit Techniques

11.1 Implementing Continuous Assurance Auditing
11.2 ACL, NetSuite, BusinessObjects, and Other Continuous Assurance Systems
11.3 Benefits of CAA
11.4 Computer-Assisted Audit Tools and Techniques
11.5 Determining the Need for CAATTs
11.6 Steps to Building Effective CAATTs
11.7 Importance of Using CAATTs for Audit Evidence Gathering
11.8 XBRL: The Internet-Based Extensible Marking Language

## Chapter 12: Control Self-Assessments and Internal Audit Benchmarking

12.1 Importance of Control Self-Assessments
12.2 CSA Model
12.3 Launching the CSA Process
12.4 Evaluating CSA Results
12.5 Benchmarking and Internal Audit
12.6 Better Understanding Internal Audit Activities

## Chapter 13: Areas to Audit: Establishing an Audit Universe and Audit Programs

13.1 Defining the Scope and Objectives of the Internal Audit Universe
13.2 Assessing Internal Audit Capabilities and Objectives
13.3 Audit Universe Time and Resource Limitations
13.4 “Selling” an Audit Universe Concept to the Audit Committee and Management
13.5 Assembling Audit Programs: Audit Universe Key Components
13.6 Audit Universe and Program Maintenance

# PART FOUR: ORGANIZING AND MANAGING INTERNAL AUDIT ACTIVITIES

## Chapter 14: Charters and Building the Internal Audit Function

14.1 Establishing an Internal Audit Function
14.2 Audit Committee and Management Authorization of an Audit Charter
14.3 Establishing an Internal Audit Function

Notes
Chapter 15: Managing the Internal Audit Universe and Key Competencies

15.1 Auditing in the Weeds: Problems with Reviews of Nonmainstream Audit Areas
15.2 Importance of an Audit Universe Schedule: What Is Right or Wrong
15.3 Importance of Internal Audit Key Competencies
15.4 Importance of Internal Audit Risk Management
15.5 Internal Auditor Interview Skills
15.6 Internal Audit Analytical and Testing Skills Competencies
15.7 Internal Auditor Documentation Skills
15.8 Recommending Results and Corrective Actions
15.9 Internal Auditor Negotiation Skills
15.10 An Internal Auditor Commitment to Learning
15.11 Importance of Internal Auditor Core Competencies

Chapter 16: Planning Audits and Understanding Project Management

16.1 The Project Management Process
16.2 PMBOK: The Project Management Book of Knowledge
16.3 PMBOK Program and Portfolio Management
16.4 Planning an Internal Audit
16.5 Understanding the Environment: Planning and Launching an Internal Audit
16.6 Audit Planning: Documenting and Understanding the Internal Control Environment
16.7 Performing Appropriate Internal Audit Procedures and Wrapping Up the Audit
16.8 Project Management Best Practices and Internal Audit Note

Chapter 17: Documenting Audit Results through Process Modeling and Workpapers

17.1 Internal Audit Documentation Requirements
17.2 Process Modeling for Internal Auditors
17.3 Internal Audit Workpapers
17.4 Workpaper Document Organization
17.5 Workpaper Preparation Techniques
17.6 Internal Audit Document Records Management
17.7 Importance of Internal Audit Documentation Notes

Chapter 18: Reporting Internal Audit Results

18.1 The Audit Report Framework
18.2 Purposes and Types of Internal Audit Reports
18.3 Published Audit Reports
18.4 Alternative Audit Report Formats
PART FIVE: IMPACT OF INFORMATION SYSTEMS ON INTERNAL AUDITING

Chapter 19: ITIL® Best Practices, the IT Infrastructure, and General Controls

19.1 Importance of IT General Controls 440
19.2 Client-Server and Small Systems General IT Controls 441
19.3 Client-Server Computer Systems 445
19.4 Small Systems Operations Internal Controls 447
19.5 Auditing IT General Controls for Small IT Systems 449
19.6 Mainframe Legacy System Components and Controls 452
19.7 Internal Control Reviews of Classic Mainframe or Legacy IT Systems 456
19.8 Legacy of Large System General Control Reviews 460
19.9 ITIL® Service Support and Delivery IT Infrastructure Best Practices 464
19.10 Service Delivery Best Practices 474
19.11 Auditing IT Infrastructure Management 482
19.12 Internal Auditor CBOK Needs for IT General Controls 483
Notes 484

Chapter 20: BYOD Practices and Social Media Internal Audit Issues

20.1 The Growth and Impact of BYOD 486
20.2 Understanding the Enterprise BYOD Environment 487
20.3 BYOD Security Policy Elements 488
20.4 Social Media Computing 492
20.5 Enterprise Social Media Computing Risks and Vulnerabilities 501
20.6 Social Media Policies 504

Chapter 21: Big Data and Enterprise Content Management

21.1 Big Data Overview 505
21.2 Big Data Governance, Risk, and Compliance Issues 509
21.3 Big Data Management, Hadoop, and Security Issues 512
21.4 Compliance Monitoring and Big Data Analytics 515
21.5 Internal Auditing in a Big Data Environment 517
21.6 Enterprise Content Management Internal Controls 517
21.7 Auditing Enterprise Content Management Processes 520
Notes 521

Chapter 22: Reviewing Application and Software Management Controls

22.1 IT Application Components 524
22.2 Selecting Applications for Internal Audit Reviews 533
26.3 Understanding the Ethics Risk Environment 633
26.4 Summarizing Ethics Survey Results: Do We Have a Problem? 637
26.5 Enterprise Codes of Conduct 637
26.6 Whistleblower and Hotline Functions 643
26.7 Auditing the Enterprise’s Ethics Functions 649
26.8 Improving Corporate Governance Practices 651
Notes 651

Chapter 27: Fraud Detection and Prevention 653
27.1 Understanding and Recognizing Fraud 655
27.2 Red Flags: Fraud Detection Signs for Internal Auditors 656
27.3 Public Accounting’s Role in Fraud Detection 659
27.4 IIA Standards for Detecting and Investigating Fraud 662
27.5 Fraud Investigations for Internal Auditors 665
27.6 Information Technology Fraud Prevention Processes 666
27.7 Fraud Detection and the Internal Auditor 669
Notes 669

Chapter 28: Internal Audit GRC Approaches and Other Compliance Requirements 671
28.1 The Road to Effective GRC Principles 672
28.2 GRC Risk Management Components 674
28.3 GRC and Internal Audit Enterprise Compliance Issues 677
28.4 Importance of Effective GRC Practices and Principles 679

PART SEVEN: THE PROFESSIONAL INTERNAL AUDITOR

Chapter 29: Professional Certifications: CIA, CISA, and More 683
29.1 Certified Internal Auditor Responsibilities and Requirements 684
29.2 Beyond the CIA: Other IIA Certifications 688
29.3 Importance of the CIA Specialty Certification Examinations 693
29.4 Certified Information Systems Auditor 694
29.5 Certified Information Security Manager 696
29.6 Certified in the Governance of Enterprise IT 696
29.7 Certified in Risk and Information Systems Control 697
29.8 Certified Fraud Examiner 697
29.9 Certified Information Systems Security Professional 698
29.10 ASQ Internal Audit Certifications 699
29.11 Other Internal Auditor Certifications 700

Chapter 30: The Modern Internal Auditor as an Enterprise Consultant 701
30.1 Standards for Internal Audit as an Enterprise Consultant 702
30.2 Launching an Internal Audit Internal Consulting Facility 704
PART EIGHT: THE OTHER SIDES OF AUDITING: PROFESSIONAL CONVERGENCE

Chapter 31: Quality Assurance Auditing and ASQ Standards 717
31.1 Duties and Responsibilities of ASQ Quality Auditors 718
31.2 Role of the Quality Auditor 720
31.3 Performing ASQ Quality Audits 723
31.4 Quality Assurance Reviews of the Internal Audit Function 727
31.5 Launching the Internal Audit Quality Assurance Review 733
31.6 Reporting the Results of an Internal Audit Quality Assurance Review 742
31.7 Future Directions for Quality Assurance Auditing 744

Chapter 32: Six Sigma and Lean Techniques for Internal Audit 745
32.1 Six Sigma Background and Concepts 746
32.2 Implementing Six Sigma 748
32.3 Six Sigma Leadership Roles and Responsibilities 749
32.4 Launching an Enterprise Six Sigma Project 752
32.5 Lean Six Sigma 754
32.6 Auditing Six Sigma Processes 757
32.7 Six Sigma in Internal Audit Operations 758
Notes 760

Chapter 33: ISO and Worldwide Internal Audit Standards 761
33.1 ISO Standards Background 762
33.2 ISO Standards Overview 764
33.3 ISO 38500 IT Governance Standard 772
33.4 ISO Standards and the COSO Internal Control Framework 776
33.5 Internal Audit and International Auditing Standards 777
Notes 779

Chapter 34: A CBOK for the Modern Internal Auditor 781
34.1 Part One: Foundations of Internal Auditing CBOK Requirements 782
34.2 Part Two: Importance of Internal Controls CBOK Requirements 783
34.3 Part Three: Planning and Performing Internal Audit CBOK Requirements 784
34.4 Part Four: Organizing and Managing Internal Audit Activities CBOK Requirements 785
34.5 Part Five: Impact of IT on Internal Auditing CBOK Requirements 786
34.6 Part Six: Internal Audit and Enterprise Governance CBOK Requirements 787
34.7 Part Seven: Internal Auditor Professional CBOK Requirements 788
34.8 Part Eight: The Other Sides of Internal Auditing: Professional Convergence CBOK Requirements 788
34.9 A CBOK for the Modern Internal Auditor 789
Notes 794

About the Author 795

Index 797