

EIGHTH
EDITION

**ROBERT
MOELLER**

**Brink's
MODERN
INTERNAL
AUDITING**

A Common Body of Knowledge

Cover design: Wiley

Copyright © 2016 by John Wiley & Sons, Inc. All rights reserved.

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

The Seventh Edition was published by Wiley in 2009.

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 for 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 publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at <http://booksupport.wiley.com>. For more information about Wiley products, visit www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Moeller, Robert R.

Brink's modern internal auditing : a common body of knowledge / Robert R. Moeller. — Eighth edition.

pages cm. — (Wiley corporate F&A)

Revised edition of the author's Brink's modern internal auditing, 2009.

Includes index.

ISBN 978-1-119-01698-4 (hardback) — ISBN 978-1-119-18000-5 (ePDF) — ISBN 978-1-119-17999-3 (ePub) — ISBN 978-1-119-18001-2 (oBook) 1. Auditing, Internal. I. Title.

HF5668.25.M64 2015

657'.458—dc23

2015023640

Printed in Singapore



M REPLACEMENT 090124 090124

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	59
4.1 COSO Internal Control Framework Principles	59
4.2 Control Environment Principle 1: Integrity and Ethical Values	60
4.3 Control Environment Principle 2: Role of the Board of Directors	64
4.4 Control Environment Principle 3: Authority and Responsibility Needs	65
4.5 Control Environment Principle 4: Commitment to a Competent Workforce	66
4.6 Control Environment Principle 5: Holding People Accountable	67
4.7 Risk Assessment Principle 6: Specifying Appropriate Objectives	68
4.8 Risk Assessment Principle 7: Identifying and Analyzing Risks	68
4.9 Risk Assessment Principle 8: Evaluating Fraud Risks	69
4.10 Risk Assessment Principle 9: Identifying Changes Affecting Internal Controls	71
4.11 Control Activities Principle 10: Selecting Control Activities That Mitigate Risks	72
4.12 Control Activities Principle 11: Selecting and Developing Technology Controls	73
4.13 Control Activities Principle 12: Policies and Procedures	74
4.14 Information and Communication Principle 13: Using Relevant, Quality Information	75
4.15 Information and Communication Principle 14: Internal Communications	78
4.16 Information and Communication Principle 15: External Communications	81
4.17 Monitoring Principle 16: Internal Control Evaluations	82
4.18 Monitoring Principle 17: Communicating Internal Control Deficiencies	83
Note	84
Chapter 5: Sarbanes-Oxley (SOx) and Beyond	85
5.1 Key Sarbanes-Oxley Act (SOx) Elements	86
5.2 Performing Section 404 Reviews under AS5	107
5.3 AS5 Rules and Internal Audit	118
5.4 Impact of the Sarbanes-Oxley Act	120
Notes	121
Chapter 6: COBIT and Other ISACA Guidance	123
6.1 Introduction to COBIT	124
6.2 COBIT Framework	126
6.3 Principle 1: Meeting Stakeholder Needs	128
6.4 Principle 2: Covering the Enterprise End to End	129
6.5 Principle 3: A Single Integrated Framework	131
6.6 Principle 4: Enabling a Holistic Approach	132
6.7 Principle 5: Separating Governance from Management	134
6.8 Using COBIT to Assess Internal Controls	135
6.9 Mapping COBIT to COSO Internal Controls	139
Notes	139

Chapter 7: Enterprise Risk Management: COSO ERM	141
7.1 Risk Management Fundamentals	142
7.2 COSO ERM: Enterprise Risk Management	153
7.3 COSO ERM Key Elements	155
7.4 Other Dimensions of COSO ERM: Enterprise Risk Objectives	171
7.5 Entity-Level Risks	174
7.6 Putting It All Together: Auditing Risk and COSO ERM Processes	175
Notes	178
PART THREE: PLANNING AND PERFORMING INTERNAL AUDITS	
Chapter 8: Performing Effective Internal Audits	181
8.1 Initiating and Launching an Internal Audit	182
8.2 Organizing and Planning Internal Audits	183
8.3 Internal Audit Preparatory Activities	184
8.4 Starting the Internal Audit	192
8.5 Developing and Preparing Audit Programs	198
8.6 Performing the Internal Audit	205
8.7 Wrapping Up the Field Engagement Internal Audit	212
8.8 Performing an Individual Internal Audit	213
Chapter 9: Standards for the Professional Practice of Internal Auditing	215
9.1 What Is the IPPF?	216
9.2 The Internal Auditing Professional Practice Standards: A Key IPPF Component	217
9.3 Content of the IIA Standards	219
9.4 Codes of Ethics: The IIA and ISACA	228
9.5 Internal Audit Principles	230
9.6 IPPF Future Directions	232
Notes	233
Chapter 10: Testing, Assessing, and Evaluating Audit Evidence	235
10.1 Gathering Appropriate Audit Evidence	236
10.2 Audit Assessment and Evaluation Techniques	236
10.3 Internal Audit Judgmental Sampling	239
10.4 Statistical Audit Sampling: An Introduction	241
10.5 Developing a Statistical Sampling Plan	247
10.6 Audit Sampling Approaches	251
10.7 Attributes Sampling Audit Example	258
10.8 Attributes Sampling Advantages and Limitations	262
10.9 Monetary Unit Sampling	263
10.10 Other Audit Sampling Techniques	267
10.11 Making Efficient and Effective Use of Audit Sampling	269
Notes	271

Chapter 11: Continuous Auditing and Computer-Assisted Audit Techniques	273
11.1 Implementing Continuous Assurance Auditing	274
11.2 ACL, NetSuite, BusinessObjects, and Other Continuous Assurance Systems	280
11.3 Benefits of CAA	281
11.4 Computer-Assisted Audit Tools and Techniques	282
11.5 Determining the Need for CAATTs	284
11.6 Steps to Building Effective CAATTs	287
11.7 Importance of Using CAATTs for Audit Evidence Gathering	288
11.8 XBRL: The Internet-Based Extensible Marking Language	290
Notes	293
Chapter 12: Control Self-Assessments and Internal Audit Benchmarking	295
12.1 Importance of Control Self-Assessments	296
12.2 CSA Model	296
12.3 Launching the CSA Process	297
12.4 Evaluating CSA Results	303
12.5 Benchmarking and Internal Audit	304
12.6 Better Understanding Internal Audit Activities	312
Notes	313
Chapter 13: Areas to Audit: Establishing an Audit Universe and Audit Programs	315
13.1 Defining the Scope and Objectives of the Internal Audit Universe	316
13.2 Assessing Internal Audit Capabilities and Objectives	321
13.3 Audit Universe Time and Resource Limitations	322
13.4 "Selling" an Audit Universe Concept to the Audit Committee and Management	324
13.5 Assembling Audit Programs: Audit Universe Key Components	325
13.6 Audit Universe and Program Maintenance	330
PART FOUR: ORGANIZING AND MANAGING INTERNAL AUDIT ACTIVITIES	
Chapter 14: Charters and Building the Internal Audit Function	335
14.1 Establishing an Internal Audit Function	336
14.2 Audit Committee and Management Authorization of an Audit Charter	337
14.3 Establishing an Internal Audit Function	338
Notes	345

Chapter 15: Managing the Internal Audit Universe and Key Competencies	347
15.1 Auditing in the Weeds: Problems with Reviews of Nonmainstream Audit Areas	348
15.2 Importance of an Audit Universe Schedule: What Is Right or Wrong	351
15.3 Importance of Internal Audit Key Competencies	352
15.4 Importance of Internal Audit Risk Management	353
15.5 Internal Auditor Interview Skills	354
15.6 Internal Audit Analytical and Testing Skills Competencies	354
15.7 Internal Auditor Documentation Skills	357
15.8 Recommending Results and Corrective Actions	360
15.9 Internal Auditor Negotiation Skills	361
15.10 An Internal Auditor Commitment to Learning	363
15.11 Importance of Internal Auditor Core Competencies	363
Chapter 16: Planning Audits and Understanding Project Management	365
16.1 The Project Management Process	366
16.2 PMBOK: The Project Management Book of Knowledge	368
16.3 PMBOK Program and Portfolio Management	375
16.4 Planning an Internal Audit	378
16.5 Understanding the Environment: Planning and Launching an Internal Audit	379
16.6 Audit Planning: Documenting and Understanding the Internal Control Environment	381
16.7 Performing Appropriate Internal Audit Procedures and Wrapping Up the Audit	383
16.8 Project Management Best Practices and Internal Audit Note	386 387
Chapter 17: Documenting Audit Results through Process Modeling and Workpapers	389
17.1 Internal Audit Documentation Requirements	390
17.2 Process Modeling for Internal Auditors	391
17.3 Internal Audit Workpapers	396
17.4 Workpaper Document Organization	401
17.5 Workpaper Preparation Techniques	405
17.6 Internal Audit Document Records Management	408
17.7 Importance of Internal Audit Documentation Notes	410 410
Chapter 18: Reporting Internal Audit Results	411
18.1 The Audit Report Framework	412
18.2 Purposes and Types of Internal Audit Reports	413
18.3 Published Audit Reports	415
18.4 Alternative Audit Report Formats	425

18.5 Internal Audit Reporting Cycle	427
18.6 Internal Audit Communications Problems and Opportunities	433
18.7 Audit Reports and Understanding People in Internal Auditing	436

PART FIVE: IMPACT OF INFORMATION SYSTEMS ON INTERNAL AUDITING

Chapter 19: ITIL® Best Practices, the IT Infrastructure, and General Controls	439
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	485
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	505
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	523
22.1 IT Application Components	524
22.2 Selecting Applications for Internal Audit Reviews	533

22.3 Preliminary Steps to Performing Application Controls Reviews	534
22.4 Completing the IT Application Controls Audit	541
22.5 Application Review Example: Client-Server Budgeting System	546
22.6 Auditing Applications under Development	549
22.7 Importance of Reviewing IT Application Controls	557
Notes	558
Chapter 23: Cybersecurity, Hacking Risks, and Privacy Controls	559
23.1 Hacking and IT Network Security Fundamentals	560
23.2 Data Security Concepts	562
23.3 Importance of IT Passwords	563
23.4 Viruses and Malicious Program Code	565
23.5 System Firewall Controls	566
23.6 Social Engineering IT Risks	568
23.7 IT Systems Privacy Concerns	570
23.8 The NIST Cybersecurity Framework	572
23.9 Auditing IT Security and Privacy	576
23.10 PCI DSS Fundamentals	579
23.11 Security and Privacy in the Internal Audit Department	580
23.12 Internal Audit's Privacy and Cybersecurity Roles	584
Chapter 24: Business Continuity and Disaster Recovery Planning	585
24.1 IT Disaster and Business Continuity Planning Today	586
24.2 Auditing Business Continuity Planning Processes	588
24.3 Building the IT Business Continuity Plan	596
24.4 Business Continuity Planning and Service Level Agreements	603
24.5 Auditing Business Continuity Plans	604
24.6 Business Continuity Planning Going Forward	605
Notes	606
PART SIX: INTERNAL AUDIT AND ENTERPRISE GOVERNANCE	
Chapter 25: Board Audit Committee Communications	609
25.1 Role of the Audit Committee	610
25.2 Audit Committee Organization and Charters	611
25.3 Audit Committee's Financial Expert and Internal Audit	617
25.4 Audit Committee Responsibilities for Internal Audit	618
25.5 Audit Committee Review and Action on Significant Audit Findings	622
25.6 Audit Committee and Its External Auditors	625
25.7 Whistleblower Programs and Codes of Conduct	625
25.8 Other Audit Committee Roles	626
Note	627
Chapter 26: Ethics and Whistleblower Programs	629
26.1 Enterprise Ethics, Compliance, and Governance	630
26.2 Ethics First Steps: Developing a Mission Statement	632

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

30.3 Ensuring an Audit and Consulting Separation of Duties	707
30.4 Consulting Best Practices	708
30.5 Expanded Internal Audit Services to Management	714

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

Preface

THIS BOOK IS A COMPLETE guide and a definition of a common body of knowledge (CBOK) for the processes 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 following outline a professional CBOK and describe internal auditing today. Although it is often misused, the word *modern* beginning with the title of the first edition says a lot about this book's heritage and the contemporary practice of internal auditing. In the first edition it described a new and evolving profession. The early internal auditors were often little more than accounting clerks or clerical support staff for their external auditors. Brink envisioned them as professionals performing much broader services to management.

Due to the pervasiveness of information technology processes and the Internet in all areas of commerce, the rules for a consistent definition of internal controls, and our evolution to a truly global economy, internal auditors today must operate in an ever-changing environment. Internal auditors need increasing levels of knowledge and understanding in many areas, but sorting through what is important and what is just nice to know represents challenges for internal auditors at all levels. This newly revised eighth edition discusses modern internal auditing in terms of areas where there is a strong knowledge requirement as well as other areas where only a general level of knowledge is needed. This edition updates our three common CBOKs for the profession of internal auditing.

The practice of internal auditing is important to enterprises today worldwide, and senior management members, 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 internal auditors and how they can serve management at all levels.

The following chapters describe this 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 here are not based on surveys of what other internal auditors are doing today; they are based on this author's long-term, 40-plus years of experience in internal auditing as well as his extensive professional activities and research.