

EIGHTH
EDITION

**ROBERT
MOELLER**

**Brink's
MODERN
INTERNAL
AUDITING**

A Common Body of Knowledge

Brink's Modern Internal Auditing

Eighth Edition

The Wiley Corporate F&A series provides information, tools, and insights to corporate professionals responsible for issues affecting the profitability of their company, from accounting and finance to internal controls and performance management.

Founded in 1807, John Wiley & Sons is the oldest independent publishing company in the United States. With offices in North America, Europe, Asia, and Australia, Wiley is globally committed to developing and marketing print and electronic products and services for our customers' professional and personal knowledge and understanding.

Brink's Modern Internal Auditing

Eighth Edition

A Common Body of Knowledge

ROBERT R. MOELLER

WILEY

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 the United States of America

10 9 8 7 6 5 4 3 2 1

*Dedicated to my best friend and wife, Lois Moeller.
Lois has been my companion and partner for over 45 years,
whether we are somewhere in the world visiting an interesting historical location,
attending one of Chicago's many music and theater events,
gardening vegetables in the backyard,
or finding the right wine and cooking the produce.*

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 CAATs	284
11.6 Steps to Building Effective CAATs	287
11.7 Importance of Using CAATs 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	410
Notes	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.

The following are some of the CBOK elements found in each chapter:

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

1. **Significance of Internal Auditing in Enterprises Today.** This introductory chapter talks about the origins of internal auditing. It does not contain key CBOK information, but provides important background knowledge and history for today's internal auditor and explains what led Victor Brink to write the first edition.
2. **An Internal Audit Common Body of Knowledge.** In this chapter, we explain and expand the concept of an internal auditing CBOK and why it is important to the profession.

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

3. **The COSO Internal Control Framework.** This recently revised 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 and how to use it in internal audit assessments of internal controls.
4. **The 17 COSO Internal Control Principles.** These principles were introduced as part of the newly revised framework and provide guidance to better help internal auditors to plan and perform their reviews of internal controls.
5. **Sarbanes-Oxley Act (SOx) and Beyond.** SOx became law in the United States in 2002 and has massively changed how we assess and measure internal accounting controls almost worldwide. The chapter discusses the current status of SOx including its AS5 auditing standards and other elements of this extensive set of legislation that are particularly important to internal auditors.
6. **COBIT and Other ISACA Guidance.** In our very IT-dependent world, internal auditors need a more IT-oriented framework to help them measure and assess internal controls as part of their review efforts. The Control Objectives for Information and related Technology (COBIT) tool is important here, and all internal auditors should have a least a general understanding of this worldwide-recognized internal control framework.
7. **Enterprise Risk Management: COSO ERM.** Risk management is an important internal audit knowledge area, and internal auditors need to understand and make use of COSO Enterprise Risk Management (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 six 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.

8. **Performing Effective Internal Audits.** This chapter contains an introduction on the overall practice of planning, performing, and completing an effective internal audit. These are the steps of what it takes to perform an internal audit.
9. **Standards for the Professional Practice of Internal Auditing.** All internal auditors need to have a strong knowledge and understanding of these Institute of Internal Auditors (IIA)–issued standards. The chapter provides an overview of the more important elements of the standards and where to search for more information.
10. **Testing, Assessing, and Evaluating Audit Evidence.** A major activity in internal auditing is to examine a record or artifact of audit evidence and then to decide if it meets audit review criteria. This is a basic internal audit knowledge area that must follow internal auditing best practices.
11. **Continuous Auditing and Computer-Assisted Audit Techniques.** The ongoing growth of 24/7 systems and processes is changing the way that internal auditors should assess and evaluate internal controls. This chapter introduces online continuous monitoring tools that internal auditors should consider a key CBOK knowledge area.
12. **Control Self-Assessments and Internal Audit Benchmarking.** The IIA has developed some extensive criteria for internal auditors at any level to look at what they are doing at a point in time and then to make an assessment of that work. The chapter describes these processes as well as guidance for improving and reviewing the quality of internal audit work.
13. **Areas to Audit: Establishing an Audit Universe and Audit Programs.** There are a wide variety of areas in any enterprise that are potential candidates for review, but internal auditors should tailor that list down to what is generally known as an audit universe. The chapter provides some guidance on how to build and assess potential review areas necessary to plan and perform internal audits.

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

14. **Charters and Building the Internal Audit Function.** Best practices here cover the building and managing of 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 committee–approved audit charter.
15. **Managing the Internal Audit Universe and Key Competencies.** Beyond the knowledge and technical skills involved in understanding the COSO internal control framework and IT general controls, internal auditors must possess some core key

competencies, such as interviewing and writing skills. These apply to all levels of an internal audit function, ranging from audit management to audit staff members. The chapter will focus on some necessary CBOK skills for all levels of internal auditors.

16. **Planning Audits and 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.
17. **Documenting Audit Results through Process Modeling and Workpapers.** As another specialized internal audit skill, internal auditors need efficient and cost-effective procedures to review and document overall business processes of all types. While many alternatives are available, this chapter will introduce some good internal audit–based approaches to understand various processes and then to document that work through audit workpapers.
18. **Reporting Internal Audit Results.** Reporting the results of audit work as well as developing recommendations for corrective actions is a major task. Whether reports are developed in hard- or soft-copy formats, this chapter will suggest approaches and guidelines for producing them effectively.

Part Five: Impact of Information Systems on Internal Auditing. Internal auditors must know how to evaluate IT controls as well as how to use IT in performing their internal audits. The six chapters in this part outline some important internal audit IT–related CBOK areas.

19. **ITIL® Best Practices, the IT Infrastructure, and General Controls.** The chapter will explain processes for reviewing IT general controls, the overall controls that cover the IT infrastructure and all aspects of IT operations. In addition, the chapter will introduce the Information Technology Infrastructure Library (ITIL®), an internationally recognized set of best practices that promote a partnership between business operations and IT functions, and explain why knowledge of ITIL® is important for internal auditors.
20. **BYOD Practices and Social Media Internal Audit Issues.** The growth of the Internet, the Internet-based nature of many systems today, and our increasing personal use of smartphones and tablet devices have introduced many changes in the manner that IT systems are managed and controlled. This chapter discusses some of the issues from an internal audit perspective and areas where internal auditors should develop a good CBOK understanding.
21. **Big Data and Enterprise Content Management.** The growth of massive IT systems coupled with legal and government requirements to capture and return this system data has led to the environment known as big data. This chapter discusses some internal control concerns in this environment as well as some internal audit knowledge needs.
22. **Reviewing Application and Software Management 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 handheld and desktop procedures to larger enterprise-wide applications. This chapter will introduce some internal audit knowledge areas and some IT audit best practices.

23. **Cybersecurity, Hacking Risks, and Privacy Controls.** IT security and privacy issues are major knowledge areas that often require specialized technical skills beyond those of many internal auditors. However, this chapter will introduce some fundamental security and privacy control concepts as well as some basic internal auditor knowledge requirements in this area.
24. **Business Continuity and Disaster Recovery Planning.** Concepts such as backing up major computer files have a long internal audit–related history, with the objective of allowing the restoration of operations in the event of a calamitous interruption in IT services. This chapter will look at an expanded view of continuity planning with an emphasis on tools and procedures to get the 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 an internal audit function with its board audit committee as well as the importance of such areas as governance, risk, and compliance (GRC) issues, ethics and whistleblower procedures, and fraud investigations.

25. **Board Audit Committee Communications.** Internal audit functions report to their board of directors' audit committees, per SOx rules. While this 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.
26. **Ethics and Whistleblower Programs.** SOx requirements and other good enterprise governance practices call for these types of programs. There are many areas described here where internal audit can help make strong improvements to operations.
27. **Fraud Detection and Prevention.** Understanding how to recognize and detect fraud is an important internal audit skill. This chapter will discuss some basic fraud understanding techniques for internal auditors.
28. **Internal Audit GRC Approaches and Other Compliance Requirements.** There are numerous compliance rules impacting today's enterprises, but the overall concept of strong and effective GRC principles is particularly important. This chapter will provide internal auditors with some of the more important of these concepts for enterprise governance purposes.

Part Seven: The Professional Internal Auditor. The two 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 its enterprise organization.

29. **Professional Certifications: CIA, CISA, and More.** Certifications such as the IIA's Certified Internal Auditor (CIA) are important for building professional credentials. This chapter will look at some of the more important certifications of interest to internal auditors, along with their requirements.

30. **The Modern Internal Auditor as an Enterprise Consultant.** Until very recent times, 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, and this chapter will discuss this internal audit role and responsibility.

Part Eight: The Other Sides of Auditing: Professional Convergence. The final part will conclude with four chapters on the importance of quality assurance auditing and the impact of International Organization for Standardization (ISO) standards on internal auditors. In addition, we will conclude by summarizing our internal audit CBOK.

31. **Quality Assurance Auditing and ASQ Standards.** The more production- and process-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 more professional convergence here going forward, and the chapter will discuss ASQ internal auditing procedures and their similarity to IIA materials.

32. **Six Sigma and Lean Techniques for Internal Audit.** Enterprises worldwide have adopted techniques, such as Six Sigma, to create all levels of operational efficiencies. The chapter will look at several that should be important knowledge areas for internal auditors and will consider how some of these programs can be used to enrich and expand internal audit activities.

33. **ISO and Worldwide Internal Audit Standards.** ISO quality systems standards are becoming increasingly important to most enterprises as they operate on a worldwide basis. This chapter will discuss the ISO process and will review some of the more important of these to internal auditors, no matter where they are working. The chapter will look at some important differences in internal auditing and other related global standards and will discuss the impact of internal accounting standards on all internal auditors. Although the IIA got its start as primarily a U.S.-based organization, it has now expanded to become truly global.

34. **A CBOK for the Modern Internal Auditor.** This final chapter will summarize the various topics from other chapters that highlight areas where internal auditors should have a strong knowledge, as well as others calling for a good general but less specific understanding. The result is our proposed internal audit CBOK.

While some topics and issues may change over time, with this eighth edition we are taking a stronger and more focused view on the knowledge areas that are essential to being a successful and outstanding internal auditor today.

PART ONE

**Foundations of Modern
Internal Auditing**

Significance of Internal Auditing in Enterprises Today: An Update

THE PROFESSION OF AUDITING HAS been with us for a long time. Mesopotamian scribes in around 3000 BC utilized elaborate systems of internal controls using stone documents that contained ticks, dots, and checkmarks. Auditing has evolved over the millennia, and today we generally think of two basic types of business enterprise auditors: external and internal. An external auditor is chartered by a regulatory authority, with authority to visit an enterprise or entity to independently review and report on the results of that review. Those reviews generally cover financial statements but may involve other compliance areas. In the United States, financial external auditors are Certified Public Accountants (CPAs), who are state-licensed and follow the standards of the American Institute of Certified Public Accountants (AICPA; www.aicpa.org). However, there are many other types of external auditors in fields such as medical equipment devices, television viewer ratings, and multiple governmental areas.

Internal auditing, as discussed throughout this book, 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, information technology systems controls, or manufacturing quality processes. Most internal auditors follow high-level standards established by their prime professional enterprise, the Institute of Internal Auditors (IIA; www.theiia.org), but there are many different practices and approaches to internal auditing today due to its worldwide nature and wide range of auditing activities.

The primary objective of this book is to define and describe internal auditing as it is or should be performed today—modern internal auditing—as well as to describe a *common body of knowledge (CBOK)* for internal auditing. Because of modern internal auditing's many variations and nuances, the chapters following describe and discuss it in terms of this CBOK, the key tools and knowledge areas that all internal auditors should generally use in their internal audit activities or at least know, as well as some

other knowledge areas where internal auditors should have at least a good general understanding. These are the common practices that are essential to the profession of modern internal auditing.

An effective way to begin to understand internal auditing and its key CBOK areas is to refer to the internationally recognized internal audit professional organization, the IIA, and its published professional standards that define the practice:

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, in contrast to external auditors, outside public accountants, or other parties such as government regulators who are not directly a part of the particular enterprise.

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

- *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.
- *Appraisal* confirms the need for an evaluation that is the thrust of internal auditors as they develop their conclusions.
- *Established* confirms that internal audit is a formal, definitive function in the modern enterprise.
- *Examine and evaluate* describe the active roles of internal auditors, first for fact-finding inquiries and then for judgmental evaluations.
- *Its activities* confirm the broad jurisdictional scope of internal audit work that applies to all of the processes and activities of the modern enterprise.
- *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.
- *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 stakeholders.

As a small terminology point, the chapters following will generally use the term *enterprise* to refer to the whole company or business, and the term *organization* or *function* to reference 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 internal auditing and internal audit professionals.

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 then proceeds to implement its plans in terms of operations, it must do something to monitor the operations to assure the achievement of its established objectives. These further efforts can be thought of as *controls*. While the internal audit function is itself one of the types of controls used, there is a wide range of other organization- or 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 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 overall enterprise. Internal auditors cannot be expected to equal, let alone exceed, the technical and operational expertise pertaining to the many various activities of an enterprise. However, they can help the responsible individuals achieve more effective results by appraising existing controls and providing a basis for helping to improve them. In addition, because internal auditors often have a good knowledge and understanding of many organizational units or special activities within a total enterprise, their levels of understanding often exceed those of other people.

1.1 INTERNAL AUDITING HISTORY AND BACKGROUND

The need for effective control processes created the concept of internal auditing. Despite its ancient roots, however, 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 as well as the rest of the world had just gone through a major economic depression. As a legislative corrective action, the SEC required that all enterprises registered with it must provide financial statements certified by independent auditors. This requirement also prompted corporations to establish internal auditing departments, but with the objective primarily to assist their independent auditors. At that time, external financial auditors were focused 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.

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 Those 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 1970s, 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 internal auditing just before going 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 *Modern Internal Auditing*.

About that same time, in 1942, the IIA was launched. Its first 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 wanted to both share their experiences and gain knowledge with others in this new professional field. A profession was born that has undergone many changes over the years and has resulted in the multifaceted profession of the modern internal auditor discussed in this book.

The typical business enterprise of the 1940s, when modern internal auditing was just getting started, required a very different skill set than 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 these machines started to become useful for record-keeping and other computational and accounting functions. Similarly, enterprises had very rudimentary telephone connections where 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 often wireless telecommunications and the Internet. The increasing complexity of modern business and other enterprises has created the need for internal auditors to become ever-greater 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 those 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 himself or herself how well a particular task has been accomplished, and perhaps how it might be done better. 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