

# **Brink's Modern Internal Auditing**

**Sixth Edition**

**Robert R. Moeller**

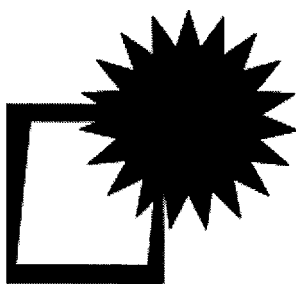


**WILEY**

**John Wiley & Sons, Inc.**



# **Brink's Modern Internal Auditing**



## Update Service

### **BECOME A SUBSCRIBER!**

*Did you purchase this product from a bookstore?*

If you did, it's important for you to become a subscriber. John Wiley & Sons, Inc. may publish, on a periodic basis, supplements and new editions to reflect the latest changes in the subject matter that you ***need to know*** in order to stay competitive in this ever-changing industry. By contacting the Wiley office nearest you, you'll receive any current update at no additional charge. In addition, you'll receive future updates and revised or related volumes on a 30-day examination review.

If you purchased this product directly from John Wiley & Sons, Inc., we have already recorded your subscription for this update service.

To become a subscriber, please call **1-877-762-2974** or send your name, company name (if applicable), address, and the title of the product to:

mailing address: **Supplement Department  
John Wiley & Sons, Inc.  
One Wiley Drive  
Somerset, NJ 08875**

e-mail: **subscriber@wiley.com**  
fax: **1-732-302-2300**  
online: **www.wiley.com**

For customers outside the United States, please contact the Wiley office nearest you:

Professional & Reference Division  
John Wiley & Sons Canada, Ltd.  
22 Worcester Road  
Etobicoke, Ontario M9W 1L1  
CANADA  
Phone: 416-236-4433  
Phone: 1-800-567-4797  
Fax: 416-236-4447  
Email: [canada@wiley.com](mailto:canada@wiley.com)

John Wiley & Sons, Ltd.  
The Atrium  
Southern Gate, Chichester  
West Sussex PO 19 8SQ  
ENGLAND  
Phone: 44-1243-779777  
Fax: 44-1243-775878  
Email: [customer@wiley.co.uk](mailto:customer@wiley.co.uk)

John Wiley & Sons Australia, Ltd.  
33 Park Road  
P.O. Box 1226  
Milton, Queensland 4064  
AUSTRALIA  
Phone: 61-7-3859-9755  
Fax: 61-7-3859-9715  
Email: [brisbane@johnwiley.com.au](mailto:brisbane@johnwiley.com.au)

John Wiley & Sons (Asia) Pte., Ltd.  
2 Clementi Loop #02-01  
SINGAPORE 129809  
Phone: 65-64632400  
Fax: 65-64634604/5/6  
Customer Service: 65-64604280  
Email: [enquiry@wiley.com.sg](mailto:enquiry@wiley.com.sg)

# **Brink's Modern Internal Auditing**

**Sixth Edition**

**Robert R. Moeller**



**WILEY**

**John Wiley & Sons, Inc.**

This book is printed on acid-free paper. ♻️

Copyright © 2005 by John Wiley & Sons, Inc. All rights reserved.

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

Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400, fax 978-646-8600, or on the web at [www.copyright.com](http://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.

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

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

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

**For more information about Wiley products, visit our Web site at [www.wiley.com](http://www.wiley.com).**

***Library of Congress Cataloging-in-Publication Data:***

Moeller, Robert R.

Brink's modern internal auditing / Robert Moeller.-- 6th ed.

p. cm.

Includes bibliographical references and index.

ISBN 0-471-67788-4 (cloth)

1. Auditing, Internal. I. Title: Modern internal auditing. II. Title.

HF5668.25.B74 2005

657'.458--dc22

2004016916

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

*To my best friend and wife,  
Lois Moeller*

## About the Author

**Robert R. Moeller** has over 25 years experience in internal auditing, ranging from launching new internal audit functions in several companies providing internal audit consulting and serving as audit director for a *Fortune* 50 corporation.

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

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

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

Robert Moeller lives with his wife, Lois, in the Chicago area. They enjoy sailing on Lake Michigan in the summer, skiing in Colorado and Utah, and participating in Chicago's theatre, opera, and music scene.

# Contents

<b>Preface</b>	<b>xix</b>
<b>PART ONE FOUNDATIONS OF INTERNAL AUDITING</b>	<b>1</b>
<b>Chapter One Foundations of Internal Auditing</b>	<b>3</b>
1.1 What is Internal Auditing?	3
1.2 Internal Auditing History and Background	4
1.3 Relationships of Operational, Financial, and Information Systems Auditing	7
<b>Chapter Two Management Needs: Internal Audit's Operational Approach</b>	<b>9</b>
2.1 Internal Audit's Management Focus	9
2.2 Operational Auditing Concepts	10
2.3 Understanding and Working with Managers and Management	11
2.4 Attributes of Management	14
2.5 Management and the Internal Auditor	17
<b>Chapter Three Internal Audit in the Twenty-First Century: Sarbanes-Oxley and Beyond</b>	<b>21</b>
3.1 Background: Changes in Financial Auditing Standards	21
3.2 "Where Were the Auditors?" Standards Failure	25
3.3 Sarbanes-Oxley Overview: Key Internal Audit Concerns	27
(a) SOA Title I: Public Company Accounting Oversight Board	29
(b) SOA Title II: Auditor Independence	39
(c) SOA Title III: Corporate Responsibility	45
(d) SOA Title IV: Enhanced Financial Disclosures	53
(e) SOA Title V: Analyst Conflicts of Interest	60
(f) SOA Titles VI and VII: Commission Authority, Studies, and Reports	61

---

Because of the rapidly changing nature of information in this field, this product may be updated with annual supplements or with future editions. **Please call 1-877-762-2974 or email us at [subscriber@wiley.com](mailto:subscriber@wiley.com) to receive any current update at no additional charge.** We will send on approval any future supplements or new editions when they become available. If you purchased this product directly from John Wiley & Sons, Inc., we have already recorded your subscription for this update service.

## CONTENTS

(g) SOA Titles VIII, IX, and X: Fraud Accountability and White-Collar Crime	62
(h) SOA Title XI: Corporate Fraud Accountability	64
3.4 Impact of the Sarbanes-Oxley Act on the Modern Internal Auditor	65
<b>PART TWO IMPORTANCE OF INTERNAL CONTROLS</b>	<b>67</b>
<b>Chapter Four Internal Controls Fundamentals: COSO Framework</b>	<b>69</b>
4.1 Importance of Effective Internal Controls	69
4.2 Fundamentals of Internal Controls	70
(a) Detective, Protective, and Corrective Control Techniques	72
4.3 Internal Controls Standards: Background Developments	74
(a) Early Definitions of Internal Control Systems	74
(b) Foreign Corrupt Practices Act of 1977	76
(c) FCPA Aftermath: What Happened?	77
4.4 Efforts Leading to the Treadway Commission	78
(a) AICPA and CICA Commissions on Auditor Responsibilities	79
(b) SEC 1979 Internal Control Reporting Proposal	80
(c) Minahan Committee and Financial Executives Research Foundation	80
(d) Earlier AICPA Standards: SAS No. 55	81
(e) Treadway Committee Report	82
4.5 COSO Internal Control Framework	83
(a) COSO Framework Model	84
4.6 Understanding, Using, and Documenting COSO Internal Controls	105
<b>Chapter Five Understanding and Assessing Risks: Enterprise Risk Management</b>	<b>107</b>
5.1 Auditing and Understanding Risks	107
5.2 Understanding Risks: COSO Enterprise Risk Management Integrated Framework	108
5.3 Enterprise Risk Management Framework	112
(a) ERM Framework Internal Environment	113
(b) Other ERM Framework Levels	116
5.4 ERM and COSO: What's the Difference?	117
5.5 Risk Ranking and Risk Assessments	118
(a) Define Organization Processes	118
(b) Rank and Score Processes Based on Relative Risk	119
(c) Assess and Identify Higher-Risk Processes	119
(d) Initiate Actions and Install Controls for Higher-Risk Processes	122
5.6 Understanding Risks for More Effective Auditing	122

## CONTENTS

<b>Chapter Six</b>	<b>Evaluating Internal Controls: Section 404 Assessments</b>	<b>123</b>
6.1	Assessments of Internal Controls after the Sarbanes-Oxley Act	123
6.2	SOA Section 404	124
	(a) Launching the Section 404 Compliance Review: Identifying Key Processes	125
	(b) Launching the Section 404 Compliance Review: Internal Audit's Role	126
	(c) Launching the Section 404 Compliance Review: Organizing the Project	127
6.3	Internal Control Review Process: Importance of Financial Assertions	138
6.4	Control Objectives and Risks under Section 404	139
	(a) Developing an Internal Controls Matrix	139
	(b) Testing Section 404 Internal Controls	142
6.5	Disclosure Committee and Keeping Section 404 Current	142
<b>Chapter Seven</b>	<b>Internal Controls Frameworks Worldwide: CobiT and Others</b>	<b>145</b>
7.1	Beyond COSO: Other Approaches to Understanding Internal Controls	145
7.2	CobiT Model: IT Governance	146
	(a) CobiT Framework	147
	(b) Navigating CobiT: Understanding the Framework	150
	(c) Control Objectives under CobiT	153
	(d) CobiT Audit Guidelines	155
	(e) Management and Implementation Guidelines	156
7.3	Using CobiT for SOA Section 404 Assessments	157
7.4	Canada's COCO Framework	161
7.5	Turnbull Report	163
7.6	Internal Control Frameworks Worldwide	164
<b>PART THREE</b>	<b>INTERNAL AUDIT AND CORPORATE GOVERNANCE</b>	<b>169</b>
<b>Chapter Eight</b>	<b>Internal Audit and the Board Audit Committee</b>	<b>171</b>
8.1	Role of the Audit Committee	171
8.2	Audit Committee Organization and Charters	173
8.3	Audit Committee's Financial Expert and Internal Audit	178
8.4	Audit Committee Responsibilities for Internal Audit	180
	(a) Appointment of the Chief Audit Executive	181
	(b) Approval of Internal Audit Charter	182
	(c) Approval of Internal Audit Plans and Budgets	183
	(d) Review and Action on Significant Audit Findings	184

## CONTENTS

8.5	Audit Committee and External Auditors	186
8.6	Whistleblower Programs and Codes of Conduct	187
8.7	Other Audit Committee Roles	188
<b>Chapter Nine Whistleblower Programs and Codes of Conduct</b>		<b>191</b>
9.1	Organizational Ethics, Compliance, and Governance	191
9.2	Launching an Organizational Ethics Program	192
	(a) First Steps: Developing a Mission Statement	193
	(b) Understanding the Risk Environment	195
	(c) Summarizing Ethics Survey Results: Do We Have a Problem?	198
9.3	Codes of Conduct	199
	(a) The Contents: What Should the Code's Message Be?	199
	(b) Communications to Stakeholders and Assuring Compliance	202
	(c) Code Violations and Corrective Actions	203
	(d) Keeping the Code Current	204
9.4	Whistleblower and Hotline Functions	205
	(a) Federal Whistleblower Rules	207
	(b) SOA Whistleblower Rules and Internal Audit	208
	(c) Launching the Organizational Help or Hotline Function	210
9.5	Auditing the Organization's Ethics Functions	211
9.6	Improving Corporate Governance Practices	213
<b>Chapter Ten Working with External Auditors</b>		<b>217</b>
10.1	Importance of External Audit Coordination	217
10.2	Professional Standards Supporting Audit Coordination	218
	(a) AICPA Support for Audit Coordination	219
	(b) Internal Audit Support for Audit Coordination	223
10.3	Internal Audit and SOA Section 404 Reviews	224
10.4	Effective Internal and External Audit Coordination	225
	(a) Problems Limiting Audit Coordination	227
10.5	Motivations for and Constraints over Effective Audit Coordination	229
10.6	Steps to Achieve Effective Audit Coordination	233
	(a) Exchange of Audit Documentation	233
	(b) Face-to-Face Sharing of Information	234
	(c) Use of a Common Methodology	235
	(d) Collaborative Work Assistance	235
	(e) Cooperation and Collaboration in Auditor Training	236
	(f) Supportive Follow-Up of Audit Findings	236
	(g) Joint Audit Project Planning	237
10.7	Coordination in Perspective	238
<b>Chapter Eleven Fraud Detection and Prevention</b>		<b>241</b>
11.1	Growing Concerns about Management Fraud	241
11.2	Red Flags: Fraud Detection for Auditors	242

## CONTENTS

11.3	Public Accounting's New Role in Fraud Detection	247
11.4	IIA Standards for Detecting and Investigating Fraud	250
11.5	Fraud Investigations for Internal Auditors	252
11.6	Information Systems Fraud Prevention Processes	253
11.7	Fraud Detection and the Auditor	255
<b>PART FOUR ADMINISTERING INTERNAL AUDIT ACTIVITIES</b>		<b>257</b>
<b>Chapter Twelve Internal Audit Professional Standards</b>		<b>259</b>
12.1	Importance of Professional Standards	259
12.2	Codes of Ethics: The IIA and ISACA	260
12.3	Internal Auditing's Professional Practice Standards	263
	(a) Background of the IIA Standards	263
	(b) IIA's Current Standards: What has Changed	264
	(c) Authority of the Internal Auditing Standards	265
12.4	Content of the IIA Standards	266
	(a) Internal Audit Attribute Standards	266
	(b) Internal Audit Performance Standards	269
	(c) Revisions to the IIA Standards	274
12.5	Importance and Relevance of the IIA Standards	274
<b>Chapter Thirteen Internal Audit Organization and Planning</b>		<b>277</b>
13.1	Organizing and Planning for the Internal Audit Function	277
13.2	Organizing the Internal Audit Effort	278
	(a) Centralized versus Decentralized Internal Audit Organizational Structures	278
	(b) Alternative Internal Audit Organization Structures	281
13.3	Internal Audit Organization Planning	286
	(a) Establishing Internal Audit Plan Goals and Objectives	287
<b>Chapter Fourteen Directing and Performing Internal Audits</b>		<b>299</b>
14.1	Organizing and Performing Internal Audits	299
14.2	Audit Planning Preparatory Activities	300
	(a) Determining Audit Objectives	301
	(b) Audit Scheduling and Time Estimates	301
	(c) Preliminary Surveys	303
14.3	Starting the Internal Audit	305
	(a) Internal Audit Field Survey	307
	(b) Documenting the Internal Audit Field Survey	309
	(c) Field Survey Auditor Conclusions	315
14.4	Using Audit Programs to Perform Internal Audits	316
	(a) Audit Program Formats and Their Preparation	318
	(b) Types of Audit Evidence	322

## CONTENTS

14.5	Performing the Internal Audit	323
	(a) Internal Audit Fieldwork Procedures	324
	(b) Audit Fieldwork Technical Assistance	326
	(c) Audit Management Fieldwork Monitoring	326
	(d) Potential Audit Findings	327
	(e) Audit Program and Schedule Modifications	328
	(f) Reporting Preliminary Audit Findings to Management	329
14.6	Planning and Controlling Internal Audit Fieldwork	330
<b>Chapter Fifteen Workpapers: Documenting Internal Audit Activities</b>		<b>333</b>
15.1	Importance of Workpapers	333
15.2	Functions of Workpapers	334
	(a) Workpaper Standards	336
	(b) Workpaper Formats	337
15.3	Workpaper Content and Organization	339
	(a) Workpaper Document Organization	339
	(b) Computer-Assisted Audit Techniques Workpapers	345
15.4	Workpaper Preparation Techniques	346
	(a) Workpaper Indexing and Cross-Referencing	346
	(b) Tick Marks	347
	(c) References to External Audit Sources	348
	(d) Workpaper Rough Notes	348
15.5	Workpaper Review Process	349
15.6	Workpaper Ownership, Custody, and Retention	350
<b>Chapter Sixteen Gathering Evidence through Audit Sampling</b>		<b>353</b>
16.1	Audit Sampling to Improve Results and Efficiency	353
16.2	Audit Sampling Decision	354
16.3	Internal Audit Judgmental Sampling	357
	(a) Judgmental Sampling Example	358
16.4	Statistical Sampling: An Introduction	362
	(a) Statistical Sampling Concepts	363
	(b) Developing a Statistical Sampling Plan	369
	(c) Selecting the Items to Be Sampled	371
16.5	Audit Sampling Approaches	374
	(a) Attribute-Sampling Procedures	375
	(b) Attribute-Sampling Audit Example	382
	(c) Attribute-Sampling Advantages and Limitations	387
16.6	Monetary Unit Sampling	388
	(a) Selecting the Monetary Unit Sample: An Example	388
	(b) Performing the Monetary Unit Sampling Test	390

## CONTENTS

(c) Evaluating Monetary Unit Sample Results	391
(d) Monetary Unit Sampling Advantages and Limitations	392
16.7 Variables and Stratified Variables Sampling	393
16.8 Other Audit Sampling Techniques	395
(a) Multistage Sampling	395
(b) Replicated Sampling	396
(c) Bayesian Sampling	396
16.9 Making Efficient and Effective Use of Audit Sampling	397
16.10 Human Resources Internal Controls Attributes Test	399
<b>Chapter Seventeen   Audit Reports and Internal                           Audit Communications</b>	<b>403</b>
17.1 Audit Reports for Effective Internal Audit Communications	403
17.2 Purposes and Types of Audit Reports	404
(a) For Whom Is the Audit Report Prepared?	405
17.3 Published Audit Report	406
(a) Approaches to Published Audit Reports	406
(b) Elements of an Audit Report Finding	411
(c) Balanced Audit Report Presentation Guidelines	415
(d) Alternative Audit Report Formats	418
17.4 Audit Reporting Cycle	420
(a) Draft Audit Reports	422
(b) Audit Reports: Follow-Up and Summarization	424
(c) Audit Report and Workpaper Retention	426
17.5 Effective Audit Communications Opportunities	427
(a) Maximizing Internal Audit Job Satisfaction	427
(b) Effective Internal Audit Communications	428
(c) Conflict and Organizational Change	430
(d) Understanding the People in Internal Auditing	432
<b>PART FIVE   IMPACT OF INFORMATION SYSTEMS                   ON INTERNAL AUDITING</b>	<b>433</b>
<b>Chapter Eighteen   Business Continuity Planning                           and Disaster Recovery</b>	<b>435</b>
18.1 Importance of Information Systems Continuity Planning	435
18.2 Business Continuity Planning Today	437
(a) Emergency Response Planning	438
(b) Business Continuity Planning	439
18.3 Continuity Planning and Service Level Agreements	441
18.4 New Business Continuity Plan Technologies: Data-Mirroring Techniques	442
18.5 Establishing Effective Contingency Policies: What Are We Protecting?	445

## CONTENTS

18.6	Building the Disaster Recovery Business Continuity Plan	447
	(a) Risks, Business Impact Analysis, and the Impact of Potential Emergencies	448
	(b) Preparing for Possible Contingencies	449
	(c) Disaster Recovery: Handling the Emergency	453
	(d) Business Continuity Plan Organization Training	453
18.7	Testing, Maintaining, and Auditing the Business Continuity Plan	454
	(a) Business Continuity Plan Testing	456
	(b) Auditing for the Effectiveness of the Business Continuation Plan	457
18.8	Continuity Planning Going Forward	459
<b>Chapter Nineteen General Controls in an E-Business and Networked Environment</b>		<b>461</b>
19.1	Importance of Information Systems General Controls	461
19.2	Mainframe, Legacy System Components, and Controls	463
	(a) Characteristics of Large Information Systems	464
	(b) Mainframe System General Controls Reviews	472
19.3	Client/Server and Small Information Systems	480
	(a) General Controls for Small Business Systems	481
	(b) Small Systems Operations Internal Controls	488
	(c) Small System Operations Internal Audit Activities	490
	(d) Small Systems Operations Controls	494
<b>Chapter Twenty Software Engineering, the Capability Maturity Model, and Project Management</b>		<b>495</b>
20.1	Capability Maturity Model and Project Management	495
20.2	The CMM Model	496
	(a) CMM Level 1: Unpredictable and Poorly Controlled Processes	497
	(b) CMM Level 2: Repeatable and Consistent Processes	499
	(c) CMM Level 3: Defined and Predictable Processes	503
	(d) CMM Level 4: Managed, Measured, and Controlled Processes	505
	(e) CMM Level 5: Optimizing Processes	506
20.3	Audit, Internal Control, and CMM	507
20.4	Information Systems Project Management	507
	(a) Project Management Integration Management	509
20.5	Project Management and the Internal Auditor	510
<b>Chapter Twenty-One Reviewing and Assessing Application Controls</b>		<b>513</b>
21.1	Importance of Information Systems Application Internal Controls	514
21.2	Components of an Information Systems Application	515
	(a) Application Input Components	516
	(b) Application Programs	519
	(c) Information Systems Output Components	523

## CONTENTS

21.3	Selecting Applications for Internal Audit Review	523
21.4	Performing the Applications Control Review: Preliminary Steps	525
	(a) Documenting Key Application Components	526
	(b) Conducting an Application Walkthrough	527
	(c) Developing Application Control Objectives	530
21.5	Completing the Information Application Control Audit	533
	(a) Understanding and Documenting Information Systems Applications	534
	(b) Clarifying and Testing Audit Control Objectives	534
	(c) Completing the Application Control Review	538
21.6	Review Example: Mainframe Accounting Application	539
	(a) Reviewing Automated Purchasing System Documentation	541
	(b) Identifying Automated Purchasing Internal Controls	542
	(c) Testing and Evaluating Automated Purchasing System Controls	542
21.7	Application–Review Example: Client/Server Budgeting	543
	(a) Reviewing Capital Budgeting System Documentation	544
	(b) Describing the Capital Budgeting Client System	544
	(c) Identifying Capital Budgeting Application Key Controls	544
	(d) Perform Application Tests of Compliance	545
21.8	Auditing Systems Under Development	546
	(a) Objectives of Preimplementation Auditing and the Obstacles	547
	(b) Preimplementation Review Procedures	550
	(c) Preimplementation Audit Reports	554
21.9	Importance of Reviewing Application Controls	555
<b>Chapter Twenty-Two Infrastructure Service- and Support-Delivery Controls</b>		<b>557</b>
22.1	Importance of Information Systems Infrastructure	557
22.2	ITIL Best Practices Model	558
	(a) ITIL Service-Support Processes	559
	(b) Service-Delivery Best Practices	570
22.3	ITIL Processes in Perspective	578
22.4	Infrastructure it Staff Support	579
<b>Chapter Twenty-Three Computer-Assisted Audit Techniques</b>		<b>581</b>
23.1	Definition of a Computer-Assisted Audit Technique	581
23.2	Determining the Need for Computer–Assisted Audit Techniques	584
23.3	Types of Computer Audit Software	588
	(a) Generalized Audit Software	588
	(b) Report Generators Languages	590
	(c) Desktop Computer Audit Software Tools	592
	(d) Test Data or “Test Deck” Approaches	593

## CONTENTS

(e) Specialized Audit Test and Analysis Software	597
(f) Embedded Audit Procedures	598
23.4 Steps to Building Effective CAATS	604
23.5 Importance of CAATS for Audit Evidence Gathering	606
<b>PART SIX INTERNAL AUDITOR TOOLS AND TRENDS</b>	<b>609</b>
<b>Chapter Twenty-Four HIPAA and Growing Concerns Regarding Privacy</b>	<b>611</b>
24.1 Beyond Sarbanes-Oxley: Growing Privacy Concerns	611
24.2 Gramm-Leach-Bliley Act	612
(a) GLBA Financial Privacy Rules	613
(b) GLBA Safeguards Rule	615
(c) GLBA Pretexting Provisions	616
24.3 Auditing for GLBA Compliance	617
24.4 HIPAA: Health-Care and Much More	618
(a) HIPAA Patient Record Privacy Rules	619
(b) Cryptography, PKI, and HIPAA Security Requirements	624
(c) HIPAA Security Administrative Procedures	624
(d) Technical Security Services and Mechanisms	626
(e) Going Forward: HIPAA and E-Commerce	627
24.5 Other Legislative Initiatives: Growing Concerns for Privacy	627
<b>Chapter Twenty-Five Continuous Assurance Auditing, XBRL, and OLAP</b>	<b>629</b>
25.1 What is Continuous Assurance Auditing?	629
25.2 Implementing Continuous Assurance Auditing	630
(a) What is a Continuous Assurance Auditing System?	631
(b) Resources for Implementing CAA	634
25.3 Internet-Based Extensible Marking Languages: XBRL	637
(a) XBRL Defined	637
(b) Implementing XBRL	638
25.4 Data Warehouses, Data Mining, and OLAP	640
(a) Importance of Storage Tools	641
(b) Data Warehouses and Data Mining	642
(c) Online Analytical Processing	644
25.5 Newer Technologies, the Continuous Close, and SOA	645
<b>Chapter Twenty-Six Internal Audit Quality-Assurance and ASQ Quality Audits</b>	<b>647</b>
26.1 ASQ Audit Standards: A Different Approach	647
26.2 Quality Auditor Standards and Practices	648
26.3 Role of the Quality Auditor	650
26.4 Quality Auditors and the IIA Internal Auditor	652

## CONTENTS

26.5	Quality-Assurance Reviews of an Internal Audit Function	652
	(a) Benefits of an Internal Audit Quality-Assurance Review	653
	(b) Elements of an Internal Audit Quality-Assurance Review	655
26.6	Launching the Internal Audit Quality-Assurance Review	659
	(a) Quality-Assurance Review Approaches	660
	(b) Example of a QA Review of an Internal Audit Function	661
	(c) Reporting the Results of an Internal Audit Quality-Assurance Review	671
26.7	Future Direction for Quality-Assurance Auditing	672
<b>Chapter Twenty-Seven Control Self-Assessments</b>		<b>675</b>
27.1	Importance of Control Self-Assessments	675
27.2	CSA Model	676
27.3	Launching the CSA Process	677
	(a) Performing the Facilitated CSA Review	678
	(b) Performing the Questionnaire-Based CSA Review	680
	(c) Performing the Management-Produced Analysis CSA Review	682
27.4	Evaluating CSA Results	682
<b>PART SEVEN THE PROFESSIONAL INTERNAL AUDITOR</b>		<b>685</b>
<b>Chapter Twenty-Eight Professional Certifications: CIA, CISA, and More</b>		<b>687</b>
28.1	Why Seek Professional Certification?	687
28.2	Certified Internal Auditor Examination	688
	(a) The CIA Examination	689
	(b) Maintaining CIA Certification	699
28.3	Other IIA-Sponsored Certifications	700
	(a) CCSA Requirements	700
	(b) CGAP <sup>®</sup> Requirements	701
	(c) CFSA Requirements	703
28.4	Certified Information Systems Auditor Examination	705
28.5	Another ISACA Certification	709
28.6	Certified Fraud Examiner Certification	709
28.7	CISSP and Information Systems Security Certification	710
28.8	ASQ Internal Audit Certifications	710
28.9	Other Certification Certifications for Internal Auditors	711
28.10	Why Get Certified for Anything?	712
<b>Chapter Twenty-Nine ISO and Internal Audit Worldwide Standards</b>		<b>713</b>
29.1	It is Not Just a United States Issue	713
29.2	SOA International Requirements	714

## CONTENTS

29.3	International Accounting and Auditing Standards	715
29.4	COSO Worldwide: International Internal Control Frameworks	722
	(a) CoCo: Canada's Equivalent of COSO	723
	(b) Internal Control Standards in the United Kingdom	724
	(c) Internal Control Frameworks Worldwide	725
29.5	ISO and the Standards Registration Process	726
	(a) ISO 9000 Quality Standards Overview	727
	(b) Quality Audits and Registration	728
29.6	ISO 9001:2000 Internal Audits	730
29.7	Another Standard: ISO 14000 Environmental Management	732
<b>Chapter Thirty Future of the Modern Internal Auditor</b>		<b>735</b>
30.1	Internal Auditing Profession Today	735
30.2	Evolving Issues and Trends	736
	(a) Importance and Significance of SOA 404 Reviews	737
	(b) Other SOA Issues: Whistleblower Programs and Internal Audit	737
	(c) PCAOB, External Audit Firms, and Internal Audit	738
	(d) Continuous Close and Information Systems Changes	739
	(e) Evolving Worldwide Standards	739
	(f) Ongoing Security and Privacy Concerns	739
30.3	Modern Internal Auditing	740
<b>Index</b>		<b>741</b>

# Preface

In 1941, the clouds of war—initiated by such dictators as Hitler, Mussolini, and Stalin—were surrounding much of the world. At the same time, Victor Z. Brink completed his New York University PhD thesis. While the “maximum leader” dictators were predicting one kind of violent revolution, Brink’s PhD thesis outlined a much more benign revolution, a revolution in the way that internal auditors should perform their work. Prior to the 1940s, internal auditors were essentially in-house assistants to their company’s public accounting firms, often performing little more than clerical financial auditing support duties for those external auditors. Brink’s thesis argued that a much better role for internal auditors should be servants to management, not external auditor assistants.

Brink then went off to service in World War II, but not before the wheels were put in place to publish his thesis as a book for business leaders. Its title was *Modern Internal Auditing*. With the United States gearing up for total war and looking to better utilize every scarce resource, the first edition of *Modern Internal Auditing* (published by John Wiley & Sons in 1942) caused many managers to consider how they might better organize their internal audit functions. Brink’s book strongly proposed that internal auditors could and should be much more significant members of an organization’s management team. The *modern* internal auditor that Brink envisioned served management by going beyond routine accounting verification procedures and taking a broader approach of *supplying service to management* as part of his or her internal audit activities.

Brink returned from the war and became director of internal audit for the Ford Motor Company. He also worked with others, such as Brad Cadmus and Larry Sawyer, to build and better define this new profession called internal auditing. A final result of the work of Brink and others was the establishment of the Institute of Internal Auditors (IIA), now a major professional accounting organization, responsible for setting standards and providing guidance to the profession of internal auditing. Often, authors of significant and groundbreaking business books “go to sleep” after their first or second editions. However, Brink kept active in the profession, revising his original 1942 edition three times over the years, either by himself or in collaboration with others in later editions.

Although Brink introduced new concepts and technologies in the subsequent editions, he never lost his basic philosophy that internal auditing should provide a basic and essential *service to management* in the modern organization. Robert Moeller took general responsibility for the fifth edition of *Modern Internal Auditing* released in 1999, and had an opportunity to meet with Vic Brink and

## PREFACE

discuss internal auditing concepts from the very early days leading to the development of that edition. Vic Brink was an impressive, interesting man, with an ongoing concern for the practice of internal auditing. This sixth edition preserves Brink's important concept of internal audit's responsibility to management but also introduces many of the changes and concepts that continue to make internal auditing exciting and important.

Each new edition of *Modern Internal Auditing* has focused on changes that were then affecting the profession of internal auditing. The fifth edition, for example, emphasized the growth of computers and information systems as a change that has very much impacted internal auditors over the last 50 to 60 years. At the time of the first edition of *Modern Internal Auditing*, the digital computer essentially did not exist and companies were just beginning to use 80- or 90-column punched-card tabulating equipment for some of their elementary statistical recordkeeping applications. There was no need to mention these machines in the first edition of this book because they were just not that important to businesses. Mainframe computers, behemoths that weighed tons and occupied major areas of floor space, were introduced in larger companies starting in the 1960s, but internal auditors initially were not concerned with them. This was the era in which audits were performed *around* the computer; that is, if a total had been generated by the computer and printed on some report, it was assumed to be correct because "the computer figured it out." Auditors were primarily concerned that the input controls were adequate. Internal auditors had little to do with these computer systems besides perhaps checking to see if the door to the computer room was locked or that candy and soft drinks were not being consumed in the computer room. The fifth edition tried to give some broad internal audit guidance in many information systems-related areas.

This sixth edition is released in the midst of a new era of concerns and responsibilities for internal auditors. The concerns regarding corporate governance, associated with the collapse of Enron Corporation, MCI, Adelphia, and others as well as the collapse of the then prominent public accounting firm, Arthur Andersen, led to the passage of the Sarbanes-Oxley Act (SOA) by the U.S. Congress in 2002. This legislation has a worldwide impact on organizations and both internal and external auditors. In many respects, SOA has given internal audit functions a level of "new respect" in the eyes of their corporate audit committees, management, the external auditors, and a much broader public.

This book has an overall objective to give the reader an overview of the many issues facing internal auditors today as well as areas of good internal audit practices. An example is the SOA Section 404 review, an internal controls document and testing process that has become a major concern for organization management today. Chapter 6, "Evaluating Internal Controls: Section 404 Assessments," provides internal audit guidance for these important SOA review requirements. In addition, an overall theme of the periodic editions has been to introduce and emphasize newer areas that should be of interest to internal auditors. The early editions of this book under Victor Brink described the operational approach to internal auditing, a major and important change from the compliance- and financial-related approaches of most internal auditors at that time. Similarly, the previous fifth edition by this author discussed such new areas of internal

## PREFACE

audit interest as the COSO (Committee of Sponsoring Organizations) internal controls framework, the importance of ethics and codes of conduct, and auditing systems under development. These were not common topics of interest for internal auditors at that time, but were areas that were believed to be of interest for the modern internal auditor. Perhaps ahead of our time, the topics on COSO internal controls as well as ethics and codes of conduct are important elements of today's SOA-driven world.

This edition continues to follow this theme of introducing newer areas of internal control or management concern that should at least be of interest to today's modern internal auditor. An example of this approach is Chapter 22, "Infrastructure Service- and Support-Delivery Controls, on the information technology infrastructure library (ITIL) standards for information systems service-delivery and service-support standards. This may become an important set of standard practices for many organizations in the future. However, in covering a broad set of topics, space does not allow for detailed discussions of areas discussed in separate chapters such as business continuity planning or audit sampling.

This edition should provide today's internal auditor with an introduction to many practices important to internal auditing. To the internal audit manager or chief audit executive (CAE), the chapters that follow are designed to give an overview of all aspects of modern internal auditing. To the staff internal auditor, the chapters are designed to give some information that should be of importance to the internal audit professional, such the previously referenced ITIL model or the Chapter 5, "Understanding and Assessing Risks: Enterprise Risk Management," discussion of the soon to be released (at the time of publication) of the COSO Enterprise Risk Management (ERM) framework.

These chapters should also be important to members of the audit committee of the board of directors as well as senior managers in the organization who deal with internal auditors on a regular basis. The chapters should provide an overview of what internal audit does, its operating practices, and the standards that create to day's profession of modern internal auditing.



---

P A R T O N E

---

**Foundations of Internal  
Auditing**



# Foundations of Internal Auditing

1.1	What is Internal Auditing?	3	1.3	Relationships of Operational, Financial, and Information Systems Auditing	7
1.2	Internal Auditing History and Background	4			

## 1.1 WHAT IS INTERNAL AUDITING?

An effective way to begin this book about modern internal auditing is to refer to the professional standards of the Institute of Internal Auditors (IIA). This internal auditor professional organization defines the practice of internal auditing as follows: *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 or other business records, or more broadly, as a thoughtful review and appraisal at the highest organizational level. In this book, we use the term *auditing* to include this total range of levels of service, from detailed checking of accounting balances to higher-level operational appraisals.

The term *internal* defines work carried on within the organization by its own employees. Internal auditing work is distinguished from such audit-related work carried on by outside public accountants or other parties (such as government regulators) who are not directly a part of an organization.

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

- *Independent* means auditing that is free of restrictions that could significantly limit the scope and effectiveness of the 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 organization.
- *Examine and evaluate* describe the active roles of internal auditors, first for fact-finding inquiries and then for judgmental evaluations.

## FOUNDATIONS OF INTERNAL AUDITING

- *Its activities* confirm the broad jurisdictional scope of internal audit work that applies to all of the activities of the modern organization.
- *Service* reveals that help and assistance to management and other members of the organization are the end products of all internal auditing work.
- *To the organization* confirms that internal audit's total service scope pertains to the entire organization, including all personnel, the board of directors and its audit committee, stockholders, and other interested stakeholders.

Internal auditing can also be recognized as an organizational control that functions by measuring and evaluating the effectiveness of other controls. When an organization establishes its planning and then proceeds to implement its plans in terms of operations, it must do something to monitor the operations to ensure 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 controls. The special role of internal audit is to help measure and evaluate those other controls. Thus, internal auditors must understand both their own role as a control function and the nature and scope of other types of controls in the organization.

Internal auditors who do their job effectively become experts in what makes for the best possible design and implementation of all types of controls. 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 control door that internal auditors come to examine and evaluate all organizational activities to provide maximum service to the organization. Internal auditors cannot be expected to equal—let alone exceed—the technical and operational expertise pertaining to the many activities of the organization. However, internal auditors can help the responsible individuals achieve more effective results by appraising existing controls and providing a basis for helping to improve those controls.

### 1.2 INTERNAL AUDITING HISTORY AND BACKGROUND

It is normal for any activity—including a control activity such as internal auditing—to come into being as a result of emerging needs. The business organization of 1942, when modern internal auditing was just getting started, was very different from our twenty-first century organization of today. For example, aside from some electromechanical devices and activities in research laboratories, computer systems did not exist. Organizations had no need for computer programmers until these machines started to become useful for various record keeping and other computational functions. Similarly, organizations 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 telecommunications and the Internet. The increasing complexity of modern business and other organizations has created the need for a similar specialist in various business controls: the internal auditor. We can better understand the nature of internal auditing today if we know something about the changing conditions in the past and the different needs these

## 1.2 INTERNAL AUDITING HISTORY AND BACKGROUND

changes created. What is the simplest or most primitive form of internal auditing and how did it come into existence? How has internal auditing responded to changing needs?

At its most primitive level, a self-assessment or internal auditing function can exist when any single person sits back and surveys something that he or she has done. At that point, the individual asks him- or herself how well a particular task has been accomplished and, perhaps, how it might be done better if it were to be done again. If a second person is involved in this activity, the assessment function would be expanded to include an evaluation of the 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 organization become more voluminous and complex, it is no longer practicable for the owner or top manager to have enough contact with every aspect of operations to satisfactorily review their effectiveness. These operations review responsibilities need to be delegated.

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

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

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

Understanding the history of internal auditing is important because this old image still persists, to some extent, for today's modern internal auditors. This is so even though the character of the internal auditing function is now very different.

Over time, the operations of various organizations increased in volume and complexity, creating managerial problems and new pressures on senior management. In response to these pressures, management recognized the possibilities for better utilization of their internal auditors. Here were individuals already set up in an audit function, and there seemed to be every good reason for getting greater value from these individuals with relatively little increase in cost.

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

In 1942, the Institute of Internal Auditors (IIA) was launched. Its first membership chapter was started in New York City, with Chicago soon to follow. The IIA was formed by people who had been given the title internal auditor by their organizations and who wanted to both share experiences and gain knowledge with others in this new professional field. A profession was born that has undergone many changes over subsequent years and has resulted in the type of modern internal auditor discussed in this book.

New business initiatives, such as the COSO (Committee of Sponsoring Organizations) internal control framework discussed in Chapter 4, "Internal Controls Fundamentals: COSO Framework," or the Sarbanes-Oxley Act (SOA) discussed in Chapter 3, "Internal Audit in the Twenty-First Century: Sarbanes-Oxley and Beyond," and Chapter 6, "Evaluating Internal Controls: Section 404 Assessments," have caused a continuing increase in the need for the services of internal auditors. In addition, some newer environmental forces have created needs in such areas as protection from industrial hazards, support of quality-control programs, and different levels of business responsibility, including ethical standards. This need for ethical standards includes higher standards for corporate governance, greater involvement of boards of directors and their audit committees, a more active role for stockholders, and a changed role for the outside public accountant.

Ethics, whistleblower programs, and codes of conduct issues will be discussed in Chapter 9, "Whistleblower Programs and Codes of Conduct." As a result of these new business directions, the services of internal auditors have become more important to a wide range of interested parties in the organization. There are now more and better-qualified internal auditing personnel and a higher level of organizational status and importance attached to them. The IIA has grown from its first, 25-member charter chapter in 1942, to an international association with over 90,000 members and hundreds of local chapters worldwide. At the same time, the importance of internal audit has been recognized by many professionals through their Standards for the Professional Practice of Internal Auditing, as will be discussed in Chapter 12, "Internal Audit Professional Standards." The internal audit profession has reached a major level of maturity and is well positioned for continuing dynamic growth.