Brink's Modern Internal Auditing

Sixth Edition

Robert R. Moeller

WILEY
John Wiley & Sons, Inc.

Contents

Preface **xix**

PART ONE FOUNDATIONS OF INTERNAL AUDITING **1**

Chapter One Foundations of Internal Auditing **3**

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

Chapter Two Management Needs: Internal Audit's Operational Approach **9**

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

Chapter Three Internal Audit in the Twenty-First Century: Sarbanes-Oxley and Beyond **21**

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}ij>OA Title I: Public Company Accounting Oversight Board 29

(b) *doA* 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* **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.

(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

PART TWO IMPORTANCE OF INTERNAL CONTROLS 67

Chapter Four Internal Controls Fundamentals: COSO Framework 69
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

Chapter Five Understanding and Assessing Risks: Enterprise Risk Management 107
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

Chapter Six Evaluating Internal Controls: Section 404 Assessments 123

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

Chapter Seven Internal Controls Frameworks Worldwide: CobiT and Others 145

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

PART THREE INTERNAL AUDIT AND CORPORATE GOVERNANCE 169

Chapter Eight Internal Audit and the Board Audit Committee 171

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

8.5 Audit Committee and External Auditors 186
8.6 Whistleblower Programs and Codes of Conduct 187
8.7 Other Audit Committee Roles 188

Chapter Nine Whistleblower Programs and Codes of Conduct 191
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

Chapter Ten Working with External Auditors 217
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

Chapter Eleven Fraud Detection and Prevention 241
11.1 Growing Concerns about Management Fraud 241
11.2 Red Flags: Fraud Detection for Auditors 242

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

PART FOUR ADMINISTERING INTERNAL AUDIT ACTIVITIES 257

Chapter Twelve Internal Audit Professional Standards 259

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

Chapter Thirteen Internal Audit Organization and Planning 277

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

Chapter Fourteen Directing and Performing Internal Audits 299

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

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

Chapter Fifteen Workpapers: Documenting Internal Audit Activities 333
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

Chapter Sixteen Gathering Evidence through Audit Sampling 353
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

(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

Chapter Seventeen Audit Reports and Internal Audit Communications 403

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

PART FIVE IMPACT OF INFORMATION SYSTEMS ON INTERNAL AUDITING 433

Chapter Eighteen Business Continuity Planning and Disaster Recovery 435

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

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

Chapter Nineteen General Controls in an E-Business and Networked Environment 461

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

Chapter Twenty Software Engineering, the Capability Maturity Model, and Project Management 495

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

Chapter Twenty-One Reviewing and Assessing Application Controls 513

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

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

Chapter Twenty-Two Infrastructure Service- and Support-Delivery Controls 557

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

Chapter Twenty-Three Computer-Assisted Audit Techniques 581

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

(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

PART SIX INTERNAL AUDITOR TOOLS AND TRENDS 609

Chapter Twenty-Four HIPAA and Growing Concerns Regarding Privacy 611
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

Chapter Twenty-Five Continuous Assurance Auditing, XBRL, and OLAP 629
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

Chapter Twenty-Six Internal Audit Quality-Assurance and ASQ Quality Audits 647
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

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

Chapter Twenty-Seven Control Self-Assessments 675

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

PART SEVEN THE PROFESSIONAL INTERNAL AUDITOR 685

Chapter Twenty-Eight Professional Certifications: CIA, CISA, and More 687

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® 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

Chapter Twenty-Nine ISO and Internal Audit Worldwide Standards 713

29.1 It is Not Just a United States Issue 713

29.2 SOA International Requirements 714

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

Chapter Thirty Future of the Modern Internal Auditor 735

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

Index 741