CONTENTS

Foreword xix
Acknowledgments xxiii
Introduction xxvii

Part I Audit Overview 1

Chapter 1 Building an Effective Internal IT Audit Function 3
Independence: The Great Myth 5
Consulting and Early Involvement 7
Four Methods for Consulting and Early Involvement 9
Early Involvement 9
Informal Audits 11
Knowledge Sharing 14
Self-Assessments 16
Final Thoughts 17
Relationship Building: Partnering vs. Policing 17
Learning to Build Partnerships 18
The Role of the IT Audit Team 21
Application Auditors 22
Data Extraction and Analysis Specialists 23
IT Auditors 24
Forming and Maintaining an Effective IT Audit Team 25
Career IT Auditors 25
IT Professionals 27
Career IT Auditors vs. IT Professionals: Final Thoughts 28
Cosourcing 30
Maintaining Expertise 30
Sources of Learning 31
Relationship with External Auditors 33
Summary 34

Chapter 2 The Audit Process 35
Internal Controls 35
Types of Internal Controls 36
Internal Control Examples 37
Determining What to Audit 38
Creating the Audit Universe 38
Ranking the Audit Universe 40
Determining What to Audit: Final Thoughts 42

The Stages of an Audit 43
Planning 43
Fieldwork and Documentation 46
Issue Discovery and Validation 47
Solution Development 48
Report Drafting and Issuance 52
Issue Tracking 58
Standards 59
Summary 59

PART II Auditing Techniques 61

Chapter 3 Auditing Entity-Level Controls 63
Background 63
Test Steps for Auditing Entity-Level Controls 64
Knowledge Base 82
Master Checklist 82
Auditing Entity-Level Controls 82

Chapter 4 Auditing Data Centers and Disaster Recovery 85
Background 85
Data Center Auditing Essentials 85
Physical Security and Environmental Controls 87
System and Site Resiliency 88
Data Center Operations 89
Disaster Preparedness 89
Test Steps for Auditing Data Centers 89
Neighborhood and External Risk Factors 90
Physical Access Controls 93
Environmental Controls 98
Power and Electricity 100
Fire Suppression 103
Data Center Operations 106
System Resiliency 111
Data Backup and Restore 112
Disaster Recovery Planning 113
Knowledge Base 115
Master Checklists 116
Auditing Data Centers 116

Chapter 5 Auditing Routers, Switches, and Firewalls 119
Background 119
Network Auditing Essentials 120
Protocols 120
OSI Model 121
Routers and Switches 122
Firewalls 124

Auditing Switches, Routers, and Firewalls 126
General Network Equipment Audit Steps 126
Additional Switch Controls: Layer 2 133
Additional Router Controls: Layer 3 136
Additional Firewall Controls 138
Tools and Technology 139
Knowledge Base 140
Master Checklists 140
General Network Equipment Audit Steps 140
Auditing Layer 2 Devices: Additional Controls for Switches ... 141
Auditing Layer 3 Devices: Additional Controls for Routers 142
Auditing Firewalls: Additional Controls 142

Chapter 6 Auditing Windows Operating Systems 143
Background 143
Windows Auditing Essentials 144
Command-Line Tips 145
Essential Command-Line Tools 145
Common Commands 146
Server Administration Tools 146
Performing the Audit 148
Test Steps for Auditing Windows 148
Setup and General Controls 148
Review Services, Installed Applications, and Scheduled Tasks .. 151
Account Management and Password Controls 154
Review User Rights and Security Options 158
Network Security and Controls 159
Network Vulnerability Scanning and Intrusion Prevention 162
How to Perform a Simplified Audit of a Windows Client 164
Tools and Technology 167
Knowledge Base 168
Master Checklists 168
Auditing Windows Servers 169
Auditing Windows Clients 170

Chapter 7 Auditing Unix and Linux Operating Systems 171
Background 171
Unix and Linux Auditing Essentials 172
Key Concepts 173
File System Layout and Navigation 173
File System Permissions 176
Users and Authentication 177
Network Services 180
Test Steps for Auditing Unix and Linux 180
Account Management and Password Controls 181
File Security and Controls 191
Network Security and Controls 197

Audit Logs 207
Security Monitoring and General Controls 210
Tools and Technology 212
Nessus 212
NMAP 213
Chkrootkit 213
Crack and John the Ripper 213
Tiger and TARA 213
Shell/Awk/etc 213
Knowledge Base 214
Master Checklists 215
Auditing Account Management and Password Controls 215
Auditing File Security and Controls 216
Auditing Network Security and Controls 216
Auditing Audit Logs 217
Auditing Security Monitoring and General Controls 217

Chapter 8 Auditing Web Servers and Web Applications 219
Background 219
Web Auditing Essentials 219
One Audit with Multiple Components 220
Part 1: Test Steps for Auditing the Host Operating System 221
Part 2: Test Steps for Auditing Web Servers 221
Part 3: Test Steps for Auditing Web Applications 224
Additional Steps for Auditing Web Applications 232
Tools and Technology 234
Knowledge Base 235
Master Checklists 236
Auditing Web Servers 236
Auditing Web Applications 236

Chapter 9 Auditing Databases 237
Background 237
Database Auditing Essentials 238
Common Database Vendors 238
Database Components 241
Test Steps for Auditing Databases 245
Setup and General Controls 246
Operating System Security 247
Account and Permissions Management 249
Data Encryption 255
Monitoring and Management 256
Tools and Technology 258
Auditing Tools 258
Monitoring Tools 258
Knowledge Base 259

Master Checklist 261
Auditing Databases 261

Chapter 10 Auditing Storage 263
Background 263
Storage Auditing Essentials 264
Key Storage Components 264
Key Storage Concepts 267
Test Steps for Auditing Storage 269
Setup and General Controls 270
Account Management 271
Storage Management 272
Additional Security Controls 274
Knowledge Base 276
Master Checklists 277

Chapter 11 Auditing Virtualized Environments 279
Background 279
Commercial and Open Source Projects 280
Virtualization Auditing Essentials 280
Test Steps for Auditing Virtualization 282
Setup and General Controls 282
Account and Resource Provisioning and Deprovisioning 284
Virtual Environment Management 285
Additional Security Controls 288
Knowledge Base 292
Hypervisors 292
Tools 292
Master Checklists 293

Chapter 12 Auditing WLAN and Mobile Devices 295
Background 295
WLAN Background 295
Data-Enabled Mobile Devices Background 298
WLAN and Mobile Device Auditing Essentials 298
Test Steps for Auditing Wireless LANs 299
Part 1: WLAN Technical Audit 299
Part 2: WLAN Operational Audit 304
Test Steps for Auditing Mobile Devices 306
Part 1: Mobile Device Technical Audit 307
Part 2: Mobile Device Operational Audit 309
Additional Considerations 311
Tools and Technology 311
Knowledge Base 312
Master Checklists 312
Auditing Wireless LANs 312
Auditing Mobile Devices 312

Chapter 13 Auditing Applications 315
Background 315
Application Auditing Essentials 316
Generalized Frameworks 316
Best Practices 319
Test Steps for Auditing Applications 321
Input Controls 321
Interface Controls 323
Audit Trails 324
Access Controls 325
Software Change Controls 329
Backup and Recovery 331
Data Retention and Classification and User Involvement 332
Operating System, Database, and Other Infrastructure Controls 333
Master Checklists 334
Application Best Practices 334
Auditing Applications 334

Chapter 14 Auditing Cloud Computing and Outsourced Operations 337
Background 337
IT Systems and Infrastructure Outsourcing 338
IT Service Outsourcing 343
Other Considerations for IT Service Outsourcing 344
SAS 70 Reports 345
Test Steps for Auditing Cloud Computing and Outsourced Operations 346
Preliminary and Overview 346
Vendor Selection and Contracts 349
Data Security 351
Operations 358
Legal Concerns and Regulatory Compliance 362
Knowledge Base 364
Master Checklist 365
Auditing Cloud Computing and Outsourced Operations 365

Chapter 15 Auditing Company Projects 367
Background 367
Project Auditing Essentials 368
High-Level Goals of a Project Audit 368
Basic Approaches to Project Auditing 369
Seven Major Parts of a Project Audit 370
Test Steps for Auditing Company Projects 371
Overall Project Management 371
Project Start-up: Requirements Gathering and Initial Design 375
Detailed Design and System Development 380
Testing 381

Implementation 384
Training 386
Project Wrap-up 387
Knowledge Base 387
Master Checklists 387
Auditing Overall Project Management 388
Auditing Project Startup 388
Auditing Detailed Design and System Development 389
Auditing Testing 389
Auditing Implementation 389
Auditing Training 390
Auditing Project Wrap-up 390

PART III Frameworks, Standards, and Regulations 391

Chapter 16 Frameworks and Standards 393
Introduction to Internal IT Controls, Frameworks, and Standards 393
COSO 394
COSO Definition of Internal Control 395
Key Concepts of Internal Control 395
Internal Control—Integrated Framework 395
Enterprise Risk Management—Integrated Framework 397
Relationship Between Internal Control and Enterprise Risk-Management Publications 400
COBIT 401
COBIT Concepts 401
IT Governance 403
IT Governance Maturity Model 404
The COSO-COBIT Connection 405
COBIT 5.0 405
ITIL 407
ITIL Concepts 408
ISO 27001 408
ISO 27001 Concepts 409
NSA INFOSEC Assessment Methodology 410
NSA INFOSEC Assessment Methodology Concepts 410
Pre-assessment Phase 410
On-Site Activities Phase 411
Post-assessment Phase 411
Frameworks and Standards Trends 411
References 412

Chapter 17 Regulations 415
An Introduction to Legislation Related to Internal Controls 415
Regulatory Impact on IT Audits 416
History of Corporate Financial Regulation 416

The Sarbanes-Oxley Act of 2002 417
SOX's Impact on Public Corporations 418
Core Points of the SOX Act 418
SOX's Impact on IT Departments 420
SOX Considerations for Companies with Multiple Locations .. 421
Impact of Third-Party Services on SOX Compliance 421
Specific IT Controls Required for SOX Compliance 422
The Financial Impact of SOX Compliance on Companies 426
Gramm-Leach-Bliley Act 426
GLBA Requirements 426
Federal Financial Institutions Examination Council 428
Privacy Regulations 428
California SB 1386 429
International Privacy Laws 429
Privacy Law Trends 430
Health Insurance Portability and Accountability Act of 1996 431
HIPAA Privacy and Security Rules 431
The HITECH Act 433
HIPAA's Impact on Covered Entities 434
EU Commission and Basel II 434
Basel II Capital Accord 434
Payment Card Industry (PCI) Data Security Standard 435
PCI Impact on the Payment Card Industry 436
Other Regulatory Trends 436
References 437

Chapter 18 Risk Management **439**
Benefits of Risk Management 439
Risk Management from an Executive Perspective 439
Addressing Risk 440
Quantitative vs. Qualitative Risk Analysis 440
Quantitative Risk Analysis 441
Elements of Risk 441
Practical Application 442
Quantitative Risk Analysis in Practice 443
Common Causes for Inaccuracies 443
Qualitative Risk Analysis 445
IT Risk Management Life Cycle 445
Phase 1: Identify Information Assets 446
Phase 2: Quantify and Qualify Threats 449
Phase 3: Assess Vulnerabilities 454
Phase 4: Remediate Control Gaps 456
Phase 5: Manage Residual Risk 458
Summary of Formulas 458

Index **459**