

---

# CONTENTS AT A GLANCE

<b>Part I</b>	Audit Overview .....	1
<b>Chapter 1</b>	Building an Effective Internal IT Audit Function .....	3
<b>Chapter 2</b>	The Audit Process .....	33
<b>Part II</b>	Auditing Techniques .....	59
<b>Chapter 3</b>	Auditing Entity-Level Controls .....	61
<b>Chapter 4</b>	Auditing Data Centers and Disaster Recovery .....	83
<b>Chapter 5</b>	Auditing Switches, Routers, and Firewalls .....	113
<b>Chapter 6</b>	Auditing Windows Operating Systems .....	135
<b>Chapter 7</b>	Auditing Unix and Linux Operating Systems .....	165
<b>Chapter 8</b>	Auditing Web Servers .....	207
<b>Chapter 9</b>	Auditing Databases .....	223
<b>Chapter 10</b>	Auditing Applications .....	247
<b>Chapter 11</b>	Auditing WLAN and Mobile Devices .....	263
<b>Chapter 12</b>	Auditing Company Projects .....	283
<b>Part III</b>	Frameworks, Standards, and Regulations .....	305
<b>Chapter 13</b>	Frameworks and Standards .....	307
<b>Chapter 14</b>	Regulations .....	327
<b>Chapter 15</b>	Risk Management .....	351
	Index .....	369

---

# CONTENTS

Foreword	xix
Acknowledgments	xxi
Introduction	xxv

## **Part I** Audit Overview . . . . . 1

### **Chapter 1** Building an Effective Internal IT Audit Function . . . . . 3

Why Are We Here? (The Internal Audit Department's Mission)	3
--	---

Independence: The Great Myth	5
------------------------------	---

#### Consulting and Early Involvement:

There's More to Being an Auditor than Auditing	7
--	---

Four Methods for Consulting and Early Involvement: Your Toolkit	9
---	---

Early Involvement	9
-------------------	---

Informal Audits	12
-----------------	----

Knowledge Sharing	14
-------------------	----

Self-Assessments	17
------------------	----

Consulting and Early-Involvement Toolkit: Final Thoughts	17
--	----

Relationship Building: Partnering versus Policing	17
---	----

Learning to Build Partnerships	19
--------------------------------	----

The Role of the IT Audit Team	20
-------------------------------	----

Information Systems Auditors	22
------------------------------	----

Support for Financial Auditors	22
--------------------------------	----

IT Auditors	22
-------------	----

Forming and Maintaining an Effective IT Audit Team	23
--	----

Career IT Auditors	23
--------------------	----

IT Professionals	25
------------------	----

Career IT Auditors versus IT Professionals: Final Thoughts	26
--	----

Cosourcing	28
------------	----

Maintaining Expertise	28
-----------------------	----

Sources of Learning	29
---------------------	----

Relationship with External Auditors	30
-------------------------------------	----

Summary	31
---------	----

### **Chapter 2** The Audit Process . . . . . 33

Internal Controls	33
-------------------	----

Types of Internal Controls	34
----------------------------	----

Internal Control Examples	35
---------------------------	----

Determining What to Audit	36
---------------------------	----

Creating the Audit Universe	36
-----------------------------	----

Ranking the Audit Universe	39
----------------------------	----

Determining What to Audit: Final Thoughts	41
---	----

The Stages of an Audit .....	41
Planning .....	42
Fieldwork and Documentation .....	44
Issue Discovery and Validation .....	45
Solution Development .....	46
Report Drafting and Issuance .....	50
Issue Tracking .....	55
Standards .....	57
Summary .....	57
<b>Part II Auditing Techniques .....</b>	<b>59</b>
<b>Chapter 3 Auditing Entity-Level Controls .....</b>	<b>61</b>
Background .....	61
Test Steps .....	62
Knowledge Base .....	79
Master Checklist .....	80
Auditing Entity-Level Controls .....	80
<b>Chapter 4 Auditing Data Centers and Disaster Recovery .....</b>	<b>83</b>
Background .....	83
Data Center Auditing Essentials .....	83
Facility-Based Controls .....	84
System and Site Resiliency .....	85
Data Center Operations .....	86
Auditing Data Centers .....	86
Neighborhood and Environment .....	87
Physical Access Control .....	90
Environmental Controls .....	92
Power Continuity .....	94
Alarm Systems .....	96
Fire Suppression .....	98
Surveillance Systems .....	100
Data Center Operations .....	101
Auditing Disaster Recovery .....	106
System Resiliency .....	106
Data Backup and Restore .....	107
Disaster Recovery Planning .....	108
Knowledge Base .....	110
Master Checklists .....	110
Auditing Data Centers .....	111
Auditing Disaster Recovery .....	112

---

<b>Chapter 5 Auditing Switches, Routers, and Firewalls</b> .....	<b>113</b>
Background .....	113
Network Auditing Essentials .....	114
Switches and Routers .....	114
Firewalls .....	116
Auditing Switches, Routers, and Firewalls .....	117
General Network Equipment Audit Steps .....	118
Additional Switch Controls: Layer 2 .....	126
Additional Router Controls: Layer 3 .....	129
Additional Firewall Controls .....	130
Tools and Technologies: Auditing Networking Equipment .....	131
Knowledge Base .....	132
Master Checklists .....	132
General Network Equipment Audit Steps .....	132
Auditing Layer 2 Devices: Additional Controls for Switches .....	133
Auditing Layer 3 Devices: Additional Controls for Routers .....	133
Auditing Firewalls: Additional Controls .....	134
<b>Chapter 6 Auditing Windows Operating Systems</b> .....	<b>135</b>
Background .....	135
Windows Auditing Basics .....	136
Command-Line Tips .....	137
Essential Command-Line Tools .....	137
Common Commands .....	138
Server Administrative Tools .....	138
Performing the Audit .....	139
Windows Server Test Steps .....	140
Setup and General Controls .....	140
Review Services, Installed Applications, and Scheduled Tasks .....	143
Account Management and Password Controls .....	146
Review User Rights and Security Options .....	150
Network Security and Controls .....	151
How to Perform a Simplified Audit of a Windows Client .....	157
Tools and Technology .....	161
Knowledge Base .....	161
Master Checklists .....	162
Auditing Windows Servers .....	162
Auditing Windows Clients .....	163
<b>Chapter 7 Auditing Unix and Linux Operating Systems</b> .....	<b>165</b>
Background .....	165
Getting Around .....	166
File System Layout, Navigation, and Permissions .....	167
File System Permissions .....	169
Users and Authentication .....	170

LDAP, NIS, or NIS+	171
Network Services	172
Test Steps	172
Account Management and Password Controls	173
File Security and Controls	182
Network Security and Controls	188
Audit Logs	196
Security Monitoring and Other Controls	199
Tools and Technology	201
Nessus	201
NMAP	201
Chkrootkit	201
John the Ripper and Crack	202
Shell/Awk/etc	202
Knowledge Base	202
Master Checklists	203
Auditing Account Management and Password Controls	203
Auditing File Security and Controls	204
Auditing Network Security and Controls	205
Auditing Audit Logs	205
Auditing Security Monitoring and Other Controls	205
<b>Chapter 8 Auditing Web Servers</b>	<b>207</b>
Background	207
Web Auditing Essentials	208
Web Auditing Components	208
Auditing Web Platforms and Web Applications	209
Auditing Web Servers	209
Auditing Web Applications	213
Tools and Technologies	220
Knowledge Base	221
Master Checklists	222
Auditing Web Servers	222
Auditing Web Applications	222
<b>Chapter 9 Auditing Databases</b>	<b>223</b>
Background	223
Database Basics	224
Common Database Vendors	224
Database Components	227
Performing the Audit	231
Test Steps	232
Tools and Technology	242
Knowledge Base	244
Master Checklist	246
Auditing Databases	246

---

<b>Chapter 10 Auditing Applications</b> .....	<b>247</b>
Application Auditing Essentials .....	247
Generalized Frameworks .....	247
Best Practices .....	250
Performing the Application Audit .....	252
Part 1: Input Controls .....	252
Part 2: Interface Controls .....	254
Part 3: Audit Trails .....	255
Part 4: Access Controls .....	255
Part 5: Software Change Controls .....	259
Part 6: Backup and Recovery .....	260
Part 7: Data Retention and Classification .....	260
Part 8: Operating System, Database, and Other Infrastructure Controls .....	261
Master Checklists .....	261
Application Best Practices .....	261
Auditing Applications .....	262
<b>Chapter 11 Auditing WLAN and Mobile Devices</b> .....	<b>263</b>
WLAN and Mobile Devices Background .....	263
WLAN Background .....	263
Data-Enabled Mobile Devices Background .....	265
WLAN and Mobile Device Auditing Essentials .....	266
Performing the Wireless LAN Audit .....	267
Part 1: WLAN Technical Audit .....	267
Part 2: WLAN Operational Audit .....	273
Performing the Mobile Device Audit .....	274
Part 1: Mobile Device Technical Audit .....	275
Part 2: Mobile Device Operational Audit .....	277
Additional Considerations .....	279
Tools and Technology .....	279
Knowledge Base .....	280
Master Checklists .....	280
Auditing Wireless LANs .....	280
Auditing Mobile Devices .....	281
<b>Chapter 12 Auditing Company Projects</b> .....	<b>283</b>
Background .....	284
High-Level Goals of a Project Audit .....	284
Basic Approaches to Project Auditing .....	285
Seven Major Parts of a Project Audit .....	286
Test Steps .....	286
Overall Project Management .....	287
Project Startup: Requirements Gathering and Initial Design .....	291
Detailed Design and System Development .....	294

Testing	296
Implementation	298
Training	300
Project Wrap-up	301
Knowledge Base	301
Master Checklists	302
Auditing Overall Project Management	302
Auditing Project Startup	302
Auditing Detailed Design and System Development	303
Auditing Testing	303
Auditing Implementation	304
Auditing Training	304
Auditing Project Wrap-up	304
<b>Part III Frameworks, Standards, and Regulations</b>	<b>305</b>
<b>Chapter 13 Frameworks and Standards</b>	<b>307</b>
Introduction to Internal IT Controls, Frameworks, and Standards	307
COSO	308
COSO Definition of Internal Control	309
Key Concepts of Internal Control	309
Internal Control—Integrated Framework	309
Enterprise Risk Management—Integrated Framework	311
CoBIT	315
CoBIT Concepts	316
IT Governance	318
IT Governance Maturity Model	318
The COSO-CoBIT Connection	319
ITIL	319
ITIL Concepts	321
ISO 27001/ISO 17799/BS 7799	322
ISO 17799 Concepts	323
NSA INFOSEC Assessment Methodology	323
NSA INFOSEC Assessment Methodology Concepts	323
Pre-assessment Phase	324
On-Site Activities Phase	324
Post-assessment Phase	325
Frameworks and Standards Trends	325
References	325
<b>Chapter 14 Regulations</b>	<b>327</b>
An Introduction to Legislation Related to Internal Controls	327
Regulatory Impact on IT Audit	327
History of Corporate Financial Regulation	328

The Sarbanes-Oxley Act of 2002	328
Sarbanes-Oxley's Impact on Public Corporations	329
Core Points of the Sarbanes-Oxley Act	329
Sarbanes-Oxley's Impact on IT Departments	331
Sarbanes-Oxley Considerations for	
Companies with Multiple Locations	332
Impact of Third-Party Services	
on Sarbanes-Oxley Compliance	332
Specific IT Controls Required	
for Sarbanes-Oxley Compliance	333
The Financial Impact of Sarbanes-Oxley	
Compliance on Companies	337
Gramm-Leach-Bliley Act	338
GLBA Requirements	338
Federal Financial Institutions Examination Council	340
Privacy Regulations Such as California SB 1386	340
Impact on Companies	340
SB 1386 Impact on Internal Controls	340
International Privacy Laws	341
Privacy Law Trends	342
Health Insurance Portability and Accountability Act of 1996	342
HIPAA Privacy and Security Rules	343
HIPAA's Impact on Covered Entities	344
EU Commission and Basel II	345
Basel II Capital Accord	345
Payment Card Industry (PCI) Data Security Standard	346
PCI Impact on the Payment Card Industry	346
Other Regulatory Trends	347
References	347
<b>Chapter 15 Risk Management</b>	<b>351</b>
Benefits of Risk Management	351
Risk Analysis	351
Elements of Risk	351
Practical Application	353
Risk Analysis in Practice	354
Common Causes for Inaccuracies in Risk Analyses	354
IT Risk Management Life Cycle	356
Phase 1: Identifying Information Assets	356
Phase 2: Quantifying and Qualifying Threats	359
Phase 3: Assessing Vulnerabilities	364
Phase 4: Control Gap Remediation	366
Phase 5: Managing Ongoing Risk	367
Summary of Formulas	368
<b>Index</b>	<b>369</b>