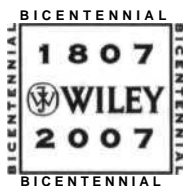


# **Auditor's Guide to Information Systems Auditing**

RICHARD E. CASCARINO



John Wiley & c Sons, Inc.

# Contents

PREFACE	xix
ABOUT THE CD	xxxiii
<b>PART I</b> .....	«
<b>IS Audit Process</b>	<b>1</b>
<b>CHAPTER 1</b>	
Technology and Audit	t
Technology and Audit	4
Batch and On-Line Systems	9
<b>CHAPTER 2</b>	
<b>IS Audit Function Knowledge</b>	<b>24</b>
Information Systems Auditing	24
What Is Management?	25
Management Process	25
Understanding the Organization's Business	26
Establishing the Needs	26
Identifying Key Activities	26
Establish Performance Objectives	27
Decide The Control Strategies	27
Implement and Monitor the Controls	27
Executive Management's Responsibility and Corporate Governance	28
Audit Role	28
Conceptual Foundation	29
Professionalism within the IS Auditing Function	29
Relationship of Internal IS Audit to the External Auditor	30
Relationship of IS Audit to Other Company Audit Activities	30
Audit Charter	30
Charter Content	31
Outsourcing the IS Audit Activity	31
Regulation, Control, and Standards	32

**CHAPTER 3**

<b>IS Risk and Fundamental Auditing Concepts</b>	<b>33</b>
Computer Risks and Exposures	33
Effect of Risk	35
Audit and Risk	37
Audit Evidence	39
Reliability of Audit Evidence	39
Audit Evidence Procedures	40
Responsibilities for Fraud Detection and Prevention	41

**CHAPTER 4**

<b>Standards and Guidelines for IS Auditing</b>	<b>48</b>
IIA Standards	43
Code of Ethics	44
Advisory	46
Aids	46
Standards for the Professional Performance of Internal Auditing	47
ISACA Standards	47
ISACA Code of Ethics	4f
COSO: Internal Control Standards	49
BS 7799 and ISO 17799: IT Security	51
NIST	53
BSI Baselines	54

**CHAPTER 5**

<b>Internal Controls Concepts Knowledge</b>	<b>87</b>
Internal Controls	57
Cost/Benefit Considerations	59
Internal Control Objectives	59
Types Of Internal Controls	61
Systems of Internal Control	62
Elements of Internal Control	63
Manual and Automated Systems	64
Control Procedures	65
Application Controls	65
Control Objectives and Risks	66
General Control Objectives	67
Data and Transactions Objectives	67
Program Control Objectives	69
Corporate IT Governance	69

**CHAPTER 6**

<b>Risk Management of the IS Function</b>	<b>71</b>
Nature of Risk	75
Auditing in General	76

Elements of Risk Analysis	78
Defining the Audit Universe	79
Computer System Threats	81
Risk Management	83
<b>CHAPTER 7</b>	
<b>Audit Planning Process</b>	<b>88</b>
Benefits of an Audit Plan	88
Structure of the Plan	93
Types of Audit	96
<b>CHAPTER 8</b>	
<b>Audit Management</b>	<b>88</b>
Planning	98
Audit Mission	99
IS Audit Mission	99
Organization of the Function	100
Staffing	101
IS Audit as a Support Function	103
Planning	103
Business Information Systems	104
Integrated IS Auditor vs Integrated IS Audit	104
Auditees as Part of the Audit Team	106
Application Audit Tools	107
Advanced Systems	107
Specialist Auditor	107
IS Audit Quality Assurance	108
<b>CHAPTER 9</b>	
<b>Audit Evidence Process</b>	<b>108</b>
Audit Evidence	109
Audit Evidence Procedures	109
Criteria for Success	110
Statistical Sampling	112
Why Sample?	112
Judgmental (or Non-Statistical) Sampling	113
Statistical Approach	114
Sampling Risk	114
Assessing Sampling Risk	116
Planning a Sampling Application	116
Calculating Sample Size	1 1 9
Quantitative Methods	122
Project Scheduling Techniques	125
Simulations	127
Computer Assisted Audit Solutions	128

Generalized Audit Software	129
Application and Industry-Related Audit Software	130
Customized Audit Software	130
Information Retrieval Software	131
Utilities	131
On-Line Inquiry	131
Conventional Programming Languages	131
Microcomputer-Based Software	132
Test Transaction Techniques	132
<b>CHAPTER 10</b>	
<b>Audit Reporting Follow-up</b>	184
Audit Reporting	134
Interim Reporting	135
Closing Conferences	135
Written Reports	135
Clear Writing Techniques	136
Preparing To Write	138
Basic Audit Report	139
Executive Summary	140
Detailed Findings	140
Polishing the Report	142
Distributing the Report	142
Follow-Up Reporting	143
Types of Follow-Up Action	144
<b>EIWJL</b>	
<b>Information Systems/Information Technology Governance</b>	145
<b>CHAPTER 11</b>	
<b>Management</b>	147
IS Infrastructures	147
Project-Based Functions	148
Quality Control	154
Operations and Production	155
Technical Services	156
Performance Measurement and Reporting	156
Measurement Implementation	158
<b>CHAPTER 12</b>	
<b>Strategic Planning</b>	164
Strategic Management Process	164
Strategic Drivers	165
New Audit Revolution	166

## Contents

Leveraging IS	166
Business Process Re-Engineering Motivation	167
IS as an Enabler of Re-Engineering	168
Dangers of Change	168
System Models	169
Information Resource Management	170
Strategic Planning for IS	171
Decision Support Systems	173
Steering Committees	174
Strategic Focus	174
Auditing Strategic Planning	175
Design the Audit Procedures	176

### CHAPTER 13

Management Issues	177
Privacy	179
Copyrights, Trademarks, and Patents	180
Ethical Issues	181
Corporate Codes of Conduct	182
IT Governance	184
Sarbanes-Oxley Act	186
Housekeeping	186

### CHAPTER 14

Support Tools and Frameworks	188
General Frameworks	188
COSO: Internal Control Standards	192
Other Standards	193

### CHAPTER 15

Governance Techniques	188
Change Control	196
Problem Management	198
Auditing Change Control	199
Operational Reviews	199
Performance Measurement	200
ISO 9000 Reviews	201

## E M M

Systems and Infrastructure Lifecycle Management	286
---	-----

### CHAPTER 16

Information Systems Planning	287
------------------------------	-----

Stakeholders	207
Operations	208
Systems Development	209
Technical Support	210
Other System Users	212
Segregation of Duties	212
Personnel Practices	214
Object-Oriented Systems Analysis	215
Enterprise Resource Planning	216
<b>CHAPTER 17</b>	
<b>Information Management and Usage</b>	218
What Are Advanced Systems ?	218
Service Delivery and Management	221
<b>CHAPTER 18</b>	
<b>Development, Acquisition, and Maintenance of Information Systems</b>	
Programming Computers	227
Program Conversions	229
System Failures	229
Systems Development Exposures	232
Systems Development Controls	233
Systems Development Life Cycle Control: Control Objectives	233
Micro-Based Systems	235
<b>CHAPTER 19</b>	
<b>Impact of Information Technology on the Business Processes and Solutions</b>	286
Impact	236
Continuous Monitoring	237
Business Process Outsourcing	238
E-Business	239
<b>CHAPTER 20</b>	
<b>Software Development</b>	241
Developing a System	241
Change Control	245
Why Do Systems Fail?	247
Auditor's Role in Software Development	249
<b>CHAPTER 21</b>	
<b>Audit and Control of Purchased Packages</b>	251
Information Systems Vendors	252
Request For Information	253
Requirements Definition	254
Request For Proposal	255

Installation	256
Systems Maintenance	257
Systems Maintenance Review	257
Outsourcing	<b>258</b>
CHAPTER 22	
Audit Role in Feasibility Studies and Conversions	258
Feasibility Success Factors	259
Conversion Success Factors	263
CHAPTER 23	
<b>Audit and Development of Application Controls</b>	<b>284</b>
What Are Systems?	264
Classifying Systems	265
Controlling Systems	266
Control Stages	266
System Models	266
Information Resource Management	267
Control Objectives of Business Systems	268
General Control Objectives	269
CAATS and their Role in Business Systems Auditing	271
Common Problems	274
Audit Procedures	274
CAAT Use in Non-Computerized Areas	275
Designing an Appropriate Audit Program	275
P*RTIW	
<b>Information Technology Service Delivery and Support</b>	<b>277</b>
CHAPTER 24	
<b>Technical Infrastructure</b>	<b>278</b>
Auditing the Technical Infrastructure	282
Computer Operations Controls	284
Operations Exposures	285
Operations Controls	286
Personnel Controls	286
Supervisory Controls	286
Operations Audits	287
CHAPTER 25	
<b>Service Center Management</b>	<b>288</b>
Continuity Management and Disaster Recovery	289
Managing Service Center Change	293



## Protection of Information Assets 285

### CHAPTER 26

Information Assets Security Management	<b>287</b>
What Is Information Systems Security?	297
Control Techniques	300
Workstation Security	301
Physical Security	301
Logical Security	301
User Authentication	
Communications Security	
Encryption	<b>102</b>
How Encryption Works	303
Encryption Weaknesses	<b>304</b>
Potential Encryption	305
Data Integrity	305
Double Public Key Encryption	<b>306</b>
Steganography	<b>307</b>
Information Security Policy	<b>308</b>

### CHAPTER 27

Logical Information Technology Security	<b>318</b>
Computer Operating Systems	310
Tailoring the Operating System	311
Auditing the Operating System	312
Security	313
Criteria	314
Security Systems: Resource Access Control Facility	314
Auditing RACF	315
Access Control Facility 2	316
Top Secret	317
User Authentication	318
Bypass Mechanisms	319

### CHAPTER 28

Applied Information Technology Security	<b>321</b>
Communications and Network Security	321
Network Protection	323
Hardening the Operating Environment	324
Client Server and Other Environments	325
Firewalls and Other Protection Resources	326
Intrusion Detection Systems	329

**CHAPTER 28**

<b>Physical and Environmental Security</b>	<b>888</b>
Control Mechanisms	332
Implementing the Controls	336

**FART VI**

<b>Business Continuity and Disaster Recovery</b>	<b>337</b>
--	------------

**CHAPTER 30**

<b>Protection of the Information Technology Architecture and Assets: Disaster Recovery Planning</b>	<b>888</b>
Risk Reassessment	341
Disaster—Before and After	341
Consequences of Disruption	343
Where to Start	344
Testing the Plan	345
Auditing the Plan	346

**CHAPTER 31**

<b>Insurance</b>	<b>348</b>
Self-Insurance	353

**PART VII**

<b>Advanced IS</b>	<b>Auditing</b>	<b>365</b>
--------------------	-----------------	------------

**CHAPTER 32**

<b>Auditing E-commerce Systems</b>	<b>387</b>
E-Commerce and Electronic Data Interchange: What Is It?	387
Opportunities and Threats	358
Risk Factors	362
Threat List	363
Security Technology	363
"Layer" Concept	363
Authentication	364
Encryption	364
Trading Partner Agreements	366
Risks and Controls within EDI and E-Commerce	366
Nonrepudiation	367
E-Commerce and Auditability	368
Compliance Auditing	369
E-Commerce Audit Approach	370

Audit Tools and Techniques	371
Auditing Security Control Structures	372
Computer Assisted Audit Techniques	372
<b>CHAPTER 33</b>	
<b>Auditing UNIX/Linux</b>	874
History	374
Security and Control in a UNIX/Linux System	377
Architecture	377
UNIX Security	378
Services	379
Daemons	380
Auditing UNIX	380
Scrutiny of Logs	381
Audit Tools in the Public Domain	381
UNIX passwd File	382
Auditing UNIX Passwords	383
<b>CHAPTER 34</b>	
<b>Auditing Windows</b>	
History	385
NT and Its Derivatives	386
Auditing Windows 23	388
Password Protection	389
File Sharing	390
Security Checklist	391
<b>CHAPTER 35</b>	
<b>Foiling the System Hackers</b>	393
<b>CHAPTER 36</b>	
<b>Investigating Information Technology Fraud</b>	387
Pre-Incident Preparation	399
Detection of Incidents	401
Initial Response	401
Forensic Backups	403
Investigation	404
Network Monitoring	404
Identity Theft	405

**APPENDICES**

<b>APPENDIX A</b>	<b>Ethics and Standards for the IS Auditor</b>	<b>407</b>
	ISACA Code of Professional Ethics	407
	Relationship of Standards to Guidelines and Procedures	408
<b>APPENDIX B</b>	<b>Audit Program for Application Systems Auditing</b>	<b>410</b>
<b>APPENDIX C</b>	<b>Logical Access Control Audit Program</b>	<b>432</b>
<b>APPENDIX D</b>	<b>Audit Program for Auditing UNIX/Linux Environments</b>	<b>446</b>
<b>APPENDIX E</b>	<b>Audit Program for Auditing Windows XP/2000 Environments</b>	<b>454</b>
	Index	463