

Contents

Preface xvii

PART I: IT AUDIT PROCESS 1

Chapter 1: Technology and Audit 3

Technology and Audit	4
Batch and Online Systems	8
Electronic Data Interchange	20
Electronic Business	21
Cloud Computing	22

Chapter 2: IT Audit Function Knowledge 25

Information Technology Auditing	25
What Is Management?	26
Management Process	26
Understanding the Organization's Business	27
Establishing the Needs	27
Identifying Key Activities	27
Establish Performance Objectives	27
Decide the Control Strategies	27
Implement and Monitor the Controls	28
Executive Management's Responsibility and Corporate Governance	28
Audit Role	28
Conceptual Foundation	29
Professionalism within the IT Auditing Function	29
Relationship of Internal IT Audit to the External Auditor	30
Relationship of IT Audit to Other Company Audit Activities	30
Audit Charter	30
Charter Content	30
Outsourcing the IT Audit Activity	31
Regulation, Control, and Standards	31

Chapter 3: IT Risk and Fundamental Auditing Concepts	33
Computer Risks and Exposures	33
Effect of Risk	35
Audit and Risk	36
Audit Evidence	37
Conducting an IT Risk-Assessment Process	38
NIST SP 800 30 Framework	38
ISO 27005	39
The "Cascarino Cube"	39
Reliability of Audit Evidence	44
Audit Evidence Procedures	45
Responsibilities for Fraud Detection and Prevention	46
Notes	46
Chapter 4: Standards and Guidelines for IT Auditing	47
IIA Standards	47
Code of Ethics	48
Advisory	48
Aids	48
Standards for the Professional Performance of Internal Auditing	48
ISACA Standards	49
ISACA Code of Ethics	50
COSO: Internal Control Standards	50
BS 7799 and ISO 17799: IT Security	52
NIST	53
BSI Baselines	54
Note	55
Chapter 5: Internal Controls Concepts Knowledge	57
Internal Controls	57
Cost/Benefit Considerations	59
Internal Control Objectives	59
Types of Internal Controls	60
Systems of Internal Control	61
Elements of Internal Control	61
Manual and Automated Systems	62
Control Procedures	63
Application Controls	63
Control Objectives and Risks	64
General Control Objectives	64
Data and Transactions Objectives	64
Program Control Objectives	66
Corporate IT Governance	66
COSO and Information Technology	68
Governance Frameworks	70
Notes	71

Chapter 6: Risk Management of the IT Function	73
Nature of Risk	73
Risk-Analysis Software	74
Auditing in General	75
Elements of Risk Analysis	77
Defining the Audit Universe	77
Computer System Threats	79
Risk Management	80
Notes	83
Chapter 7: Audit Planning Process	85
Benefits of an Audit Plan	85
Structure of the Plan	89
Types of Audit	91
Chapter 8: Audit Management	93
Planning	93
Audit Mission	94
IT Audit Mission	94
Organization of the Function	95
Staffing	95
IT Audit as a Support Function	97
Planning	97
Business Information Systems	98
Integrated IT Auditor versus Integrated IT Audit	98
Auditees as Part of the Audit Team	100
Application Audit Tools	100
Advanced Systems	100
Specialist Auditor	101
IT Audit Quality Assurance	101
Chapter 9: Audit Evidence Process	103
Audit Evidence	103
Audit Evidence Procedures	103
Criteria for Success	104
Statistical Sampling	105
Why Sample?	106
Judgmental (or Non-Statistical) Sampling	106
Statistical Approach	107
Sampling Risk	107
Assessing Sampling Risk	108
Planning a Sampling Application	109
Calculating Sample Size	111
Quantitative Methods	111
Project-Scheduling Techniques	116
Simulations	117

Computer-Assisted Audit Solutions	118
Generalized Audit Software	118
Application and Industry-Related Audit Software	119
Customized Audit Software	120
Information-Retrieval Software	120
Utilities	120
On-Line Inquiry	120
Conventional Programming Languages	120
Microcomputer-Based Software	121
Test Transaction Techniques	121
Chapter 10: Audit Reporting Follow-up	123
Audit Reporting	123
Interim Reporting	124
Closing Conferences	124
Written Reports	124
Clear Writing Techniques	125
Preparing to Write	126
Basic Audit Report	127
Executive Summary	127
Detailed Findings	128
Polishing the Report	129
Distributing the Report	129
Follow-up Reporting	129
Types of Follow-up Action	130
PART II: INFORMATION TECHNOLOGY GOVERNANCE	131
Chapter 11: Management	133
IT Infrastructures	133
Project-Based Functions	134
Quality Control	138
Operations and Production	139
Technical Services	140
Performance Measurement and Reporting	140
Measurement Implementation	141
Notes	145
Chapter 12: Strategic Planning	147
Strategic Management Process	147
Strategic Drivers	148
New Audit Revolution	149
Leveraging IT	149
Business Process Re-Engineering Motivation	150
IT as an Enabler of Re-Engineering	151
Dangers of Change	152
System Models	152

Information Resource Management	153
Strategic Planning for IT	153
Decision Support Systems	155
Steering Committees	156
Strategic Focus	156
Auditing Strategic Planning	156
Design the Audit Procedures	158
Note	158
Chapter 13: Management Issues	159
Privacy	161
Copyrights, Trademarks, and Patents	162
Ethical Issues	162
Corporate Codes of Conduct	163
IT Governance	164
Sarbanes-Oxley Act	166
Payment Card Industry Data Security Standards	166
Housekeeping	167
Notes	167
Chapter 14: Support Tools and Frameworks	169
General Frameworks	169
COSO: Internal Control Standards	172
Other Standards	173
Governance Frameworks	176
Note	178
Chapter 15: Governance Techniques	179
Change Control	179
Problem Management	181
Auditing Change Control	181
Operational Reviews	182
Performance Measurement	182
ISO 9000 Reviews	184
PART III: SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT	185
Chapter 16: Information Systems Planning	187
Stakeholders	187
Operations	188
Systems Development	189
Technical Support	189
Other System Users	191
Segregation of Duties	191
Personnel Practices	192
Object-Oriented Systems Analysis	194

Enterprise Resource Planning	194
Cloud Computing	195
Notes	197
Chapter 17: Information Management and Usage	199
What Are Advanced Systems?	199
Service Delivery and Management	201
Computer-Assisted Audit Tools and Techniques	204
Notes	205
Chapter 18: Development, Acquisition, and Maintenance of Information Systems	207
Programming Computers	207
Program Conversions	209
No Thanks Systems Development Exposures	209
Systems Development Controls	210
Systems Development Life Cycle Control: Control Objectives	210
Micro-Based Systems	212
Cloud Computing Applications	212
Note	213
Chapter 19: Impact of Information Technology on the Business Processes and Solutions	215
Impact	215
Continuous Monitoring	216
Business Process Outsourcing	218
E-Business	219
Notes	220
Chapter 20: Software Development	221
Developing a System	221
Change Control	225
Why Do Systems Fail?	225
Auditor's Role in Software Development	227
Chapter 21: Audit and Control of Purchased Packages and Services	229
IT Vendors	230
Request For Information	231
Requirements Definition	231
Request for Proposal	232
Installation	233
Systems Maintenance	233
Systems Maintenance Review	234
Outsourcing	234
SAS 70 Reports	234

Chapter 22: Audit Role in Feasibility Studies and Conversions	237
Feasibility Success Factors	237
Conversion Success Factors	240
Chapter 23: Audit and Development of Application Controls	243
What Are Systems?	243
Classifying Systems	244
Controlling Systems	244
Control Stages	245
Control Objectives of Business Systems	245
General Control Objectives	246
CAATs and Their Role in Business Systems Auditing	247
Common Problems	249
Audit Procedures	250
CAAT Use in Non-Computerized Areas	250
Designing an Appropriate Audit Program	250
PART IV: INFORMATION TECHNOLOGY SERVICE DELIVERY AND SUPPORT	253
Chapter 24: Technical Infrastructure	255
Auditing the Technical Infrastructure	257
Infrastructure Changes	259
Computer Operations Controls	260
Operations Exposures	261
Operations Controls	261
Personnel Controls	261
Supervisory Controls	262
Information Security	262
Operations Audits	263
Notes	264
Chapter 25: Service-Center Management	265
Private Sector Preparedness (PS Prep)	266
Continuity Management and Disaster Recovery	266
Managing Service-Center Change	269
Notes	269
PART V: PROTECTION OF INFORMATION ASSETS	271
Chapter 26: Information Assets Security Management	273
What Is Information Systems Security?	273
Control Techniques	276
Workstation Security	276

Physical Security	276
Logical Security	277
User Authentication	277
Communications Security	277
Encryption	277
How Encryption Works	278
Encryption Weaknesses	279
Potential Encryption	280
Data Integrity	280
Double Public Key Encryption	281
Steganography	281
Information Security Policy	282
Notes	282
Chapter 27: Logical Information Technology Security	283
Computer Operating Systems	283
Tailoring the Operating System	284
Auditing the Operating System	285
Security	286
Criteria	286
Security Systems: Resource Access Control Facility	287
Auditing RACF	288
Access Control Facility 2	289
Top Secret	290
User Authentication	291
Bypass Mechanisms	293
Security Testing Methodologies	293
Notes	295
Chapter 28: Applied Information Technology Security	297
Communications and Network Security	297
Network Protection	298
Hardening the Operating Environment	300
Client Server and Other Environments	301
Firewalls and Other Protection Resources	301
Intrusion-Detection Systems	303
Note	304
Chapter 29: Physical and Environmental Security	305
Control Mechanisms	306
Implementing the Controls	310

PART VI: BUSINESS CONTINUITY AND DISASTER RECOVERY 311

Chapter 30: Protection of the Information Technology Architecture and Assets: Disaster-Recovery Planning 313

Risk Reassessment	314
Disaster—Before and After	315
Consequences of Disruption	317
Where to Start	317
Testing the Plan	319
Auditing the Plan	320

Chapter 31: Displacement Control 323

Insurance	323
Self-Insurance	327

PART VII: ADVANCED IT AUDITING 329

Chapter 32: Auditing E-commerce Systems 331

E-Commerce and Electronic Data Interchange: What Is It?	331
Opportunities and Threats	332
Risk Factors	335
Threat List	335
Security Technology	336
“Layer” Concept	336
Authentication	336
Encryption	337
Trading Partner Agreements	338
Risks and Controls within EDI and E-Commerce	338
E-Commerce and Auditability	340
Compliance Auditing	340
E-Commerce Audit Approach	341
Audit Tools and Techniques	341
Auditing Security Control Structures	342
Computer-Assisted Audit Techniques	343
Notes	343

Chapter 33: Auditing UNIX/Linux 345

History	345
Security and Control in a UNIX/Linux System	347
Architecture	348
UNIX Security	348
Services	349
Daemons	350
Auditing UNIX	350
Scrutiny of Logs	351
Audit Tools in the Public Domain	351

UNIX Password File	352
Auditing UNIX Passwords	353
Chapter 34: Auditing Windows VISTA and Windows 7	355
History	355
NT and Its Derivatives	356
Auditing Windows Vista/Windows 7	357
Password Protection	358
VISTA/Windows 7	359
Security Checklist	359
Chapter 35: Foiling the System Hackers	361
Chapter 36: Preventing and Investigating Information Technology Fraud	367
Preventing Fraud	367
Investigation	369
Identity Theft	376
Note	376
Appendix A Ethics and Standards for the IS Auditor	377
ISACA Code of Professional Ethics	377
Relationship of Standards to Guidelines and Procedures	378
Appendix B Audit Program for Application Systems Auditing	379
Appendix C Logical Access Control Audit Program	393
Appendix D Audit Program for Auditing UNIX/Linux Environments	401
Appendix E Audit Program for Auditing Windows VISTA and Windows 7 Environments	407
About the Author	415
About the Website	417
Index	419