Contents

PREFACE xix

ABOUT THE CD xxxiii

PART I

IS Audit Process 1

CHAPTER 1

Technology and Audit 3

Technology and Audit 4

Batch and On-Line Systems 9

CHAPTER 2

IS Audit Function Knowledge 24

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

COPYRIGHTED MATERIAL

http://www.pbookshop.com

CHAPTER 3
IS Risk and Fundamental Auditing Concepts **33**
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
Standards and Guidelines for IS Auditing **43**
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 49
COSO: Internal Control Standards 49
BS 7799 and ISO 17799: IT Security 51
NIST 53
BSI Baselines 54

CHAPTER 5
Internal Controls Concepts Knowledge **57**
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 68
Corporate IT Governance 69

CHAPTER 6
Risk Management of the IS Function **75**
Nature of Risk 75
Auditing in General 76

http://www.pbookshop.com

Elements of Risk Analysis 78
Defining the Audit Universe 79
Computer System Threats 81
Risk Management 83

CHAPTER 7
Audit Planning Process **88**
Benefits of an Audit Plan 88
Structure of the Plan 93
Types of Audit 96

CHAPTER 8
Audit Management **98**
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

CHAPTER 9
Audit Evidence Process **109**
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 119
Quantitative Methods 122
Project Scheduling Techniques 125
Simulations 127
Computer Assisted Audit Solutions 128

http://www.pbookshop.com

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

CHAPTER 10
Audit Reporting Follow-up 134
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

PART II
Information Systems/Information Technology Governance 145

CHAPTER 11
Management 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

CHAPTER 12
Strategic Planning 164
Strategic Management Process 164
Strategic Drivers 165
New Audit Revolution 166

http://www.pbookshop.com

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

PART III
Systems and Infrastructure Lifecycle Management **205**

CHAPTER 16
Information Systems Planning **207**

http://www.pbookshop.com

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

CHAPTER 17
Information Management and Usage 218
What Are Advanced Systems? 218
Service Delivery and Management 221

CHAPTER 18
Development, Acquisition, and Maintenance of Information Systems 227
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

CHAPTER 19
Impact of Information Technology on the Business Processes and Solutions 236
Impact 236
Continuous Monitoring 237
Business Process Outsourcing 238
E-Business 239

CHAPTER 20
Software Development 241
Developing a System 241
Change Control 245
Why Do Systems Fail? 247
Auditor's Role in Software Development 249

CHAPTER 21
Audit and Control of Purchased Packages 251
Information Systems Vendors 252
Request For Information 253
Requirements Definition 254
Request For Proposal 255

http://www.pbookshop.com

Installation 256
Systems Maintenance 257
Systems Maintenance Review 257
Outsourcing 258

CHAPTER 22
Audit Role in Feasibility Studies and Conversions 259
Feasibility Success Factors 259
Conversion Success Factors 263

CHAPTER 23
Audit and Development of Application Controls 264
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

PART IV
Information Technology Service Delivery and Support 277

CHAPTER 24
Technical Infrastructure 279
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
Service Center Management 289
Continuity Management and Disaster Recovery 289
Managing Service Center Change 293

http://www.pbookshop.com

PART V

Protection of Information Assets 295

CHAPTER 26

Information Assets Security Management 297
What Is Information Systems Security? 297
Control Techniques 300
Workstation Security 301
Physical Security 301
Logical Security 301
User Authentication 302
Communications Security 302
Encryption 302
How Encryption Works 303
Encryption Weaknesses 304
Potential Encryption 305
Data Integrity 305
Double Public Key Encryption 306
Steganography 307
Information Security Policy 308

CHAPTER 27

Logical Information Technology Security 310
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 321
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

http://www.pbookshop.com

CHAPTER 29
Physical and Environmental Security **330**
Control Mechanisms 332
Implementing the Controls 336

PART VI
Business Continuity and Disaster Recovery **337**

CHAPTER 30
Protection of the Information Technology Architecture and Assets: Disaster Recovery Planning **339**
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
Insurance **349**
Self-Insurance 353

PART VII
Advanced IS Auditing **355**

CHAPTER 32
Auditing E-commerce Systems **357**
E-Commerce and Electronic Data Interchange: What Is It? 357
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

http://www.pbookshop.com

Audit Tools and Techniques 371
Auditing Security Control Structures 372
Computer Assisted Audit Techniques 372

CHAPTER 33
Auditing UNIX/Linux 374
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

CHAPTER 34
Auditing Windows 385
History 385
NT and Its Derivatives 386
Auditing Windows 23 388
Password Protection 389
File Sharing 390
Security Checklist 391

CHAPTER 35
Foiling the System Hackers 393

CHAPTER 36
Investigating Information Technology Fraud 397
Pre-Incident Preparation 399
Detection of Incidents 401
Initial Response 401
Forensic Backups 403
Investigation 404
Network Monitoring 404
Identity Theft 405

http://www.pbookshop.com

APPENDICES

APPENDIX A Ethics and Standards for the IS Auditor 407
ISACA Code of Professional Ethics 407
Relationship of Standards to Guidelines and Procedures 408

APPENDIX B Audit Program for Application Systems Auditing 410

APPENDIX C Logical Access Control Audit Program 432

APPENDIX D Audit Program for Auditing UNIX/Linux Environments 446

APPENDIX E Audit Program for Auditing Windows XP/2000 Environments 454

Index 463

http://www.pbookshop.com

http://www.pbookshop.com