

Contents

<i>Introduction</i>	<i>xix</i>
<i>Assessment Test</i>	<i>xxxvii</i>
Chapter 1	Secrets of a Successful IS Auditor
	1
Demands for IS Audit	2
Understanding Policies, Standards, Guidelines, and Procedures	3
Understanding the ISACA Code of Professional Ethics	4
Understanding the Purpose of an Audit	6
Understanding the Auditor's Responsibility	6
Auditor Role vs. Auditee Role	6
Applying an Independence Test	7
Understanding the Various Auditing Standards	8
Identifying the Types of Audits	11
Auditor Is an Executive Position	12
Understanding the Importance of Auditor Confidentiality	13
Working with Lawyers	14
Retaining Audit Documentation	14
Providing Good Communication and Integration	15
Understanding Leadership Duties	15
Planning and Setting Priorities	16
Providing Standard Terms of Reference	17
Dealing with Conflicts and Failures	17
Identifying the Value of Internal and External Auditors	18
Understanding the Evidence Rule	18
Identifying Who You Need to Interview	19
Understanding the Corporate Organizational Structure	21
Identifying Roles in a Corporate Organizational Structure	21
Identifying Roles in a Consulting Firm	
Organizational Structure	22
Managing Projects	23
What Is a Project?	25
What Is Project Management?	26
Identifying the Requirements of a Project Manager	27
Identifying a Project Manager's Authority	27
Understanding the Project Management	
Process Framework	28
Using Project Management Diagramming Techniques	37
Summary	38

xii Contents

	Exam Essentials	39
	Review Questions	41
	Answers to Review Questions	45
Chapter 2	Audit Process	47
	Establishing and Approving an Audit Charter	48
	Role of the Audit Committee	50
	Engagement Letter	51
	Preplanning the Audit	51
	Identifying Restrictions on Scope	53
	Planning Detailed Audit Objectives	54
	Risk Management Strategy	55
	Performing an Audit Risk Assessment	57
	Determining Whether an Audit Is Possible	58
	Performing the Audit	59
	Allocating Staffing	59
	Ensuring Audit Quality Control	60
	Defining Auditee Communications	60
	Using Data Collection Techniques	61
	Reviewing Existing Controls	63
	Identifying Audit Evidence	65
	Types of Evidence	65
	Grading Evidence	66
	Timing of Evidence	67
	Evidence Life Cycle	68
	Typical Evidence for IS Audits	70
	Using Evidence to Prove a Point	71
	Preparing Audit Documentation	71
	Selecting Audit Samples	72
	Identifying Audit Testing	73
	Using Computer Assisted Audit Tools	74
	Detecting Irregularities and Illegal Acts	76
	Reporting Your Audit Findings	78
	Identifying Omitted Procedures	79
	Conducting an Exit Interview	79
	Conducting Follow-Up Activities	79
	Traditional Audit Compared to Control	
	Self-Assessments	80
	Summary	80
	Exam Essentials	81
	Review Questions	83
	Answers to Review Questions	87

Chapter 3	IT Governance	89
	Strategy in Organizational Control	90
	Overview of the IT Steering Committee	91
	Selecting an IT Strategy	96
	Specifying a Policy	96
	Planning the IT Strategy	98
	Identifying Sourcing Locations	100
	Conducting an Executive Performance Review	103
	Understanding the Auditor's Interest in the Strategy	103
	Overview of Tactical Management	103
	Planning and Performance	104
	Management Control Methods	104
	Project Management	107
	Risk Management	107
	Implementing Standards	109
	Human Resources	111
	System Life-Cycle Management	112
	Continuity Planning	112
	Insurance	112
	Performance Management	113
	Overview of Business Process Reengineering	114
	Why Use Business Process Reengineering	114
	BPR Goals	115
	BPR Principles	115
	BPR Steps	116
	Benchmarking as a BPR Tool	116
	BPR Project Risk Assessment	117
	Business Process Controls to Consider	118
	Knowledge Requirements for BPR	119
	The Practical Application of BPR	119
	Conducting a Business Impact Analysis	121
	Practical Selection Methods for BPR	123
	A Practical Approach to the BPR Project	124
	Tactical Management	127
	Operations Management	127
	Supporting IT Goals	127
	Sustaining Operations	128
	Understanding Personnel Roles and Responsibilities	128
	Using Compensating Controls	132
	Tracking Performance	132
	Controlling Change	133
	Understanding the Auditor's Interest in Operational Delivery	133

	Summary	134
	Exam Essentials	134
	Review Questions	136
	Answers to Review Questions	140
Chapter 4	Networking Technology	143
	Understanding the Differences in Computer Architecture	144
	Comparing Single Processor and Multiprocessor Systems	148
	Identifying Various Operating Systems	148
	Selecting the Best Computer	151
	Comparing Computer Capabilities	153
	Processing vs. System Control	154
	Dealing with Data Storage	155
	Protecting Port Controls and Port Access	157
	Overview of the Open Systems Interconnect (OSI) Model	158
	Layer 1: Physical Layer	160
	Layer 2: Data-Link Layer	160
	Layer 3: Network Layer	162
	Layer 4: Transport Layer	164
	Layer 5: Session Layer	164
	Layer 6: Presentation Layer	165
	Layer 7: Application Layer	166
	Understanding How Computers Communicate	167
	Physical Network Design	168
	Overview of Network Topologies	169
	Identifying Bus Topologies	169
	Identifying Star Topologies	169
	Identifying Ring Topologies	171
	Identifying Meshed Networks	171
	Network Cable Types	173
	Unshielded Twisted-Pair (UTP) Cable	173
	Coaxial Cable	174
	Fiber-Optic Cable	174
	Network Devices	174
	Network Services	177
	Domain Name Service	177
	Dynamic Host Configuration Protocol	177
	Expanding the Network	180
	Wireless Access Solutions	183
	Summarizing the Various Area Networks	185
	Managing Your Network	186
	Syslog	186
	Automated Cable Tester	187

	Protocol Analyzer	187
	Simple Network Management Protocol	187
	Remote Monitoring Protocol Version 2	188
	Summary	188
	Exam Essentials	189
	Review Questions	191
	Answers to Review Questions	195
Chapter 5	Life Cycle Management	197
	Governance in Software Development	198
	Managing Software Quality	199
	Capability Maturity Model	199
	International Organization for Standardization	200
	Overview of Steering Committees	202
	Identifying Critical Success Factors	202
	Using the Scenario Approach	203
	Aligning Software to Business Needs	203
	Change Management	206
	Managing the Software Project	207
	Choosing an Approach	207
	Using Traditional Project Management	208
	Overview of the System Development Life Cycle	210
	Phase 1: Feasibility Study	212
	Phase 2: Requirements Definition	215
	Phase 3: System Design	218
	Phase 4: Development	219
	Phase 5: Implementation	227
	Phase 6: Post-implementation	230
	Overview of Data Architecture	231
	Databases	231
	Database Transaction Integrity	236
	Decision Support Systems	236
	Presenting DSS Data	238
	Using Artificial Intelligence	238
	Program Architecture	238
	Centralization vs. Decentralization	239
	Electronic E-commerce	239
	Summary	240
	Exam Essentials	240
	Review Questions	243
	Answers to Review Questions	247

Chapter 6	IT Service Delivery	249
	IT Operations	250
	Using the IT Balanced Scorecard	252
	Using Metrics	253
	Help Desk	256
	Service-Level Management	256
	Monitoring Controls	257
	System Access Controls	257
	Data File Controls	259
	Application Processing Controls	260
	Maintenance Controls	262
	Change Management	262
	Software Release and Patch Management	263
	Configuration Control	264
	Change Authorization	264
	Emergency Changes	264
	Management Controls	264
	System Monitoring	266
	Network Management	266
	Capacity Management	266
	Problem Management	267
	IT Performance Indicators	268
	Summary	268
	Exam Essentials	269
	Review Questions	270
	Answers to Review Questions	274
Chapter 7	Information Asset Protection	277
	Understanding the Threat	278
	Examples of Threats and Computer Crimes	279
	Identifying the Perpetrators	281
	Overview of Attack Methods	283
	Using Administrative Protection	288
	Information Security Management	288
	IT Security Governance	289
	Authority Roles over Data	290
	Identify Data Retention Requirements	291
	Document Access Paths	291
	Personnel Management	292
	Implementing Physical Protection	295
	Data Processing Locations	296
	Environmental Controls	296
	Safe Storage	302

	Using Technical Protection	303
	Technical Control Classification	304
	Application Software Controls	304
	Authentication Methods	305
	Network Access Protection	311
	Intrusion Detection	317
	Encryption Methods	321
	Public-Key Infrastructure	325
	Network Security Protocols	327
	Design for Redundancy	328
	Telephone Security	329
	Technical Self-Assessment	330
	Summary	330
	Exam Essentials	330
	Review Questions	332
	Answers to Review Questions	336
Chapter 8	Disaster Recovery and Business Continuity	339
	Defining Disaster Recovery	340
	Surviving Financial Challenges	340
	Valuing Brand Names	341
	Rebuilding after a Disaster	341
	Defining the Purpose of Business Continuity	341
	Uniting Other Plans with Business Continuity	344
	Identifying the Business Continuity Planning Phases	345
	Phase 1—Initiation	348
	Phase 2—Risk Analysis	350
	Phase 3—Business Impact Analysis (BIA)	354
	Phase 4—Strategy Selection	356
	Phase 5—Emergency Response	362
	Phase 6—Plan Creation	365
	Phase 7—Training and Awareness	369
	Phase 8—Maintain and Test	369
	Phase 9—Crisis Communications	370
	Phase 10—Integration with Other Plans	372
	Summary	372
	Exam Essentials	373
	Review Questions	375
	Answers to Review Questions	379
	Glossary	381
	<i>Index</i>	407