

 WILEY

TIMELY. PRACTICAL. RELIABLE.

The CISA[®] Prep Guide

Mastering
the Certified
Information
Systems
Auditor Exam



John B. Kramer



Contents

Introduction	xi
Chapter 1 The Information System Audit Process	1
IS Auditing Standards	2
Risk-Based Approach	6
Know Your Business	7
Controls	9
Preventive Controls	9
Detective Controls	9
Corrective Controls	9
Types of Audit Engagements	11
SAS 70	12
The Audit Organization	13
Audit Planning	15
Materiality	16
Irregularities	16
Scheduling	18
Self-Assessment Audits	19
Audit Staffing	19
Planning the Individual Audit	20
IS Audit Types	21
Risk Assessment	22
CobiT	24
Audit Objectives and Scope	28
Using the Work of Other Auditors	29
Impact of Outsourcing on IS Audits	30
Independence of an Auditor	30
Audit Engagement	31

Contents

Creating and Maintaining Work Papers	32
Due Care	33
Cover Sheet	33
Key Documents	34
Background	34
Planning and Risk Assessment	35
Audit Program	35
Test Work and Evidence	36
Post-Audit Checklist	37
Fieldwork	37
Control Objectives and Audit Approach	37
Referencing	38
Obtaining Evidence to Achieve the Audit Objectives	38
Flowcharts	39
Documentation Reviews	39
Narratives	40
Interview	40
Observation	40
Inspection	41
Confirmation	41
Reperformance	41
Monitoring	42
Test Work	42
CAATs	43
Management Control Reports	44
Sampling	44
Preparing Exhibits	47
Identifying Conditions and Defining Reportable Findings	47
Conclusions	48
Identification of Control Weaknesses	49
Summarizing Identified Weaknesses into Findings	49
Root Cause Analysis	50
Value-Added Recommendations	50
Reasonable Assurance through a Review of Work	51
The AIC and the Next Level Review of the Work Performed	51
Peer Review	52
Communicating Audit Results and Facilitating Change	52
Report Layout	53
Findings	54
Responses	55
Follow-Up	56
Resources	56
Publication	56
Web Sites	56
Sample Questions	57

Chapter 2	Management, Planning, and Organization of Information Systems	65
	Evaluate the IS Strategy and Alignment with the Business Objectives	66
	Systems Architecture	68
	Evaluate the IS Organizational Structure	69
	Roles and Responsibilities	69
	Qualification and Training of the IS Staff	73
	Evaluating IS Policies, Standards, and Procedures	75
	Policy	75
	Standards	78
	Procedures	78
	Evaluating Third-Party Services Selection and Management	79
	Contract Management	81
	Service Level Agreements	82
	Evaluating Project Management	83
	Evaluating Change Management	85
	Evaluating Problem Management	87
	Evaluating Quality Management	88
	System Development Life Cycle (SDLC)	89
	Quality Assurance Standards and Procedures	93
	Evaluating Performance Management	94
	Key Performance Indicators (KPIs)	94
	Performance Measurement Techniques	95
	Evaluating Capacity Management	97
	Economic Performance Practices	97
	Evaluating Information Security Management	100
	Evaluating Business Continuity Management	103
	Evaluating IS Management Practices and Policy Compliance	106
	Resources	107
	Sample Questions	108
Chapter 3	Technical Infrastructure and Operational Practices	115
	Evaluating Systems Software	116
	Operating Systems	116
	Database Management Systems	120
	Multi-Tier Client/Server Configuration Implications	123
	Security Packages	125
	Operations Management Consoles	128
	Evaluating Hardware Acquisition, Installation, and Maintenance	131
	Installation	134
	Maintenance	135
	Evaluating Network Infrastructure	137
	Voice Networks	137
	Data Networks	141

Contents

Evaluating IS Operational Practices	147
Computer Operations	148
Printer Operators	150
Media Library Management	151
Physical Access to Operations Areas	154
Help Desk and User Support	155
Job Scheduling	156
Configuration Management	158
Asset Management	159
Change Management	160
Evaluating System Performance	164
Monitoring Techniques, Processes, and Tools	164
Capacity Planning	166
Problem Management	168
Service Level Agreements (SLAs)	169
Resources	171
Sample Questions	172
Chapter 4 Protection of Information Assets	179
Security Risks and Review Objectives	181
The Security Officer's Role	183
Privacy Risk	186
The Security Program	187
Policy and Standards	189
Periodic Security Assessments and Planning	195
Designing Security from the Start	197
Identification, Authentication, and Authorization	198
Need to Know	200
Security Controls Economics	201
Role-Based Access	202
Evaluating Account Administration	204
User Account Management	205
Single Sign-On Solutions	208
Application Design Security	209
Application and Data Access	210
Information Ownership and Custodianship	212
Evaluating Logical Access Controls	215
Good Passwords	215
Strong Authentication	218
PKI and Digital Signatures	219
Biometric Access Controls	222
Network User Access	223
Information Security Architecture	224
Security Plans and Compliance	225
Host-Based Security	230

Evaluating Network Infrastructure Security	238
Firewalls	240
Demilitarized Zones (DMZs)	244
Proxies	246
Evaluating Encryption Techniques	247
Virtual Private Networks (VPNs)	249
Web Access Controls	251
Email Security	255
Virus Protection	256
Logging and Monitoring	259
Network Intrusion Detection	261
Incident Response	263
Security Testing Tools	265
Third-Party Connections	267
Evaluating Security Awareness	270
Social Engineering	271
Evaluating Environmental Controls	274
Electrical Power	275
Temperature	278
Fire Suppression	279
Humidity	281
Maintenance	282
Evaluating Physical Access Controls and Procedures	282
Visitor and Vendor Access	284
The Physical Location, Security Measures, and Visibility Profile	285
Personnel Safety	286
Hard Copy Information Protection	287
Resources	288
Sample Questions	289
Chapter 5 Disaster Recovery and Business Continuity	301
The Business Case for Continuity Planning	303
The Process of Planning for Adequate Recovery and Continuity	305
Evaluating Business Impact Analysis and the Requirements-Definition Processes	310
Evaluating Media and Documentation Back Up Procedures	313
Evaluating Recovery Plans, Documentation, and Maintenance	317
Evaluating Alternative Business Processing Plans and Associated Training	324
Business Processing Alternatives	327
Training Evaluation	329

Evaluating Testing Methods, Results Reporting, and Follow-Up Processes	331
Reporting Evaluation	334
Follow-Up	335
Resources	336
Sample Questions	337
Chapter 6 Business Application Systems Development, Acquisition, Implementation, and Maintenance	345
Evaluation Approach	347
Systems Development Approaches and Management	349
Project Management	350
Functional Requirements	351
Requirements Definitions	352
Feasibility Analysis	353
System Specifications	356
System Design	359
Quality Assurance Planning and Review Processes	363
System Development	365
Change Control Methodologies	366
Third-Party Participation	367
Documentation and Standards	368
Data Management, Security, and Audit Functionality	370
Testing and Code Promotion	379
Training	385
Concluding on the Development Process	386
Acquisition	388
Evaluate the Application System Acquisition and Implementation Process	389
Vendor Management and Escrow	392
Implementation	395
Conversion	396
Problem Management and Escalation	397
Emergency Change Management	398
Post-Implementation	399
Acceptance and Post-Implementation Review	399
Evaluating the Maintenance and Enhancement Processes	400
Versioning and Release Packaging	401
Resources	402
Sample Questions	403
Chapter 7 Business Process Evaluation and Risk Management	411
Corporate Governance	413
Evaluating the Effectiveness of the Information Systems in Supporting the Business Process	417
Best Practice Business Process Design	418
Management Controls	420

Key Performance Indicators (KPIs)	421
Evaluating Business Process Reengineering Projects	423
Assessing Performance and Customer Satisfaction	426
E-Business Applications in Support of Business	428
Evaluating the Design and Implementation of Risk Controls	431
Preventive Controls	433
Detective Controls	435
Corrective Controls	435
Automated or Programmed Controls	436
Manual Controls	436
Cost-Benefit Analysis of Control Efforts	438
Evaluating Risk Management and Governance	
Implementation	438
Risk Analysis	440
Control Identification	442
Gap Analysis and Reporting	443
Independent Assurance	445
Provisions for Independent Audits	450
Resources	456
Sample Questions	457

Appendix A Answers to Sample Exam Questions 465

Chapter 1—The IS Audit Process	465
Chapter 2—Management, Planning, and Organization of Information Systems	477
Chapter 3—Technical Infrastructure and Operational Practices	488
Chapter 4—Protection of Information Assets	499
Chapter 5—Disaster Recovery and Business Continuity	519
Chapter 6—Business Application Systems Development, Acquisition, Implementation, and Maintenance	530
Chapter 7— Business Process Evaluation and Risk Management	542

Appendix B What's on the CD-ROM 555

Index 559