
CONTENTS AT A GLANCE

Chapter 1	Becoming a CISA	1
Chapter 2	IT Governance and Risk Management	17
Chapter 3	The Audit Process	79
Chapter 4	IT Life-Cycle Management	135
Chapter 5	IT Service Delivery and Infrastructure	221
Chapter 6	Information Asset Protection	309
Chapter 7	Business Continuity and Disaster Recovery	421
Appendix A	Conducting a Professional Audit	485
Appendix B	Popular Methodologies, Frameworks, and Guidance	547
Appendix C	About the CD	571
	Glossary	573
	Index	619

CONTENTS

	Acknowledgments	xxi
	Introduction	xxiii
Chapter 1	Becoming a CISA	1
	Benefits of CISA Certification	2
	Becoming a CISA	3
	Experience Requirements	3
	Direct Work Experience	4
	Substitution of Experience	4
	ISACA Code of Professional Ethics	6
	ISACA IS Standards	6
	The Certification Exam	8
	Preparing for the Exam	9
	Before the Exam	9
	Day of the Exam	11
	After the Exam	11
	Applying for Certification	11
	Retaining Certification	12
	Continuing Education	12
	CPE Maintenance Fees	14
	Revocation of Certification	14
	CISA Exam Preparation Pointers	15
	Summary	15
Chapter 2	IT Governance and Risk Management	17
	Practices for Executives and Board of Directors	18
	IT Governance	18
	IT Strategy Committee	18
	The Balanced Scorecard	19
	Information Security Governance	20
	Enterprise Architecture	20
	IT Strategic Planning	22
	The IT Steering Committee	23
	Policy, Processes, Procedures, and Standards	24
	Information Security Policy	25
	Privacy Policy	25
	Procedures	26
	Standards	27
	Risk Management	28

	The Risk Management Program	28
	The Risk Management Process	30
	Risk Treatment	38
	IT Management Practices	40
	Personnel Management	40
	Sourcing	45
	Change Management	54
	Financial Management	54
	Quality Management	55
	Security Management	57
	Optimizing Performance	58
	Organization Structure and Responsibilities	59
	Roles and Responsibilities	61
	Segregation of Duties	66
	Auditing IT Governance	68
	Reviewing Documentation and Records	68
	Reviewing Contracts	70
	Reviewing Outsourcing	71
	Chapter Summary	72
	Chapter 2 Notes	73
	Questions	74
	Answers	76
Chapter 3	The Audit Process	79
	Audit Management	79
	The Audit Charter	79
	The Audit Program	80
	Strategic Audit Planning	80
	Audit and Technology	82
	Audit Laws and Regulations	83
	ISACA Auditing Standards	87
	ISACA Code of Professional Ethics	87
	ISACA Audit Standards	88
	ISACA Audit Guidelines	91
	ISACA Audit Procedures	98
	Risk Analysis	101
	Auditors' Risk Analysis and the Corporate Risk Management Program	101
	Evaluating Business Processes	101
	Identifying Business Risks	102
	Risk Mitigation	104
	Countermeasures Assessment	104
	Monitoring	104
	Internal Controls	105

Control Classification	105
Internal Control Objectives	107
IS Control Objectives	108
General Computing Controls	109
IS Controls	109
Performing an Audit	110
Audit Objectives	111
Types of Audits	111
Compliance vs. Substantive Testing	113
Audit Methodology	113
Audit Evidence	116
Computer-Assisted Audit	122
Reporting Audit Results	122
Other Audit Topics	124
Using External Auditors	126
Control Self-Assessment	127
Advantages and Disadvantages	127
The Self-Assessment Life Cycle	128
Self-Assessment Objectives	128
Auditors and Self-Assessment	129
Implementation of Audit Recommendations	129
Chapter Notes	130
Summary	131
Questions	132
Answers	134
Chapter 4 IT Life-Cycle Management	135
Business Realization	136
Portfolio and Program Management	136
Business Case Development	138
Measuring Business Benefits	139
Project Management	140
Organizing Projects	140
Developing Project Objectives	141
Managing Projects	142
Project Roles and Responsibilities	144
Project Planning	145
Project Management Methodologies	157
The Software Development Life Cycle (SDLC)	161
SDLC Phases	161
Software Development Risks	186
Alternative Software Development Approaches and Techniques	187
System Development Tools	190
Infrastructure Development and Implementation	191

Infrastructure	192
Maintaining Information Systems	194
The Change Management Process	195
Configuration Management	196
Business Processes	196
The Business Process Life Cycle (BPLC)	197
Capability Maturity Models	199
Application Controls	201
Input Controls	201
Processing Controls	204
Output Controls	205
Auditing the Software Development Life Cycle	206
Auditing Project Management	207
Auditing the Feasibility Study	207
Auditing Requirements	207
Auditing Design	208
Auditing Software Acquisition	208
Auditing Development	209
Auditing Testing	209
Auditing Implementation	209
Auditing Post-Implementation	210
Auditing Change Management	210
Auditing Configuration Management	210
Auditing Business Controls	211
Auditing Application Controls	211
Transaction Flow	211
Observations	211
Data Integrity Testing	212
Testing Online Processing Systems	212
Auditing Applications	213
Continuous Auditing	213
Chapter Summary	214
Chapter 4 Notes	216
Questions	217
Answers	219
Chapter 5 IT Service Delivery and Infrastructure	221
Information Systems Operations	221
Management and Control of Operations	221
IT Service Management	222
Infrastructure Operations	232
Monitoring	233
Software Program Library Management	233
Quality Assurance	234

Security Management	235
Information Systems Hardware	235
Computer Usage	235
Computer Hardware Architecture	237
Hardware Maintenance	244
Hardware Monitoring	245
Information Systems Architecture and Software	245
Computer Operating Systems	245
Data Communications Software	247
File Systems	247
Database Management Systems	248
Media Management Systems	252
Utility Software	252
Network Infrastructure	253
Network Architecture	254
Network-Based Services	256
Network Models	258
Network Technologies	268
Local Area Networks	269
Wide Area Networks	277
Wireless Networks	280
The TCP/IP Suite of Protocols	283
The Global Internet	293
Network Management	296
Networked Applications	297
Auditing IS Infrastructure and Operations	299
Auditing IS Hardware	299
Auditing Operating Systems	299
Auditing File Systems	300
Auditing Database Management Systems	300
Auditing Network Infrastructure	301
Auditing Network Operating Controls	302
Auditing IS Operations	302
Auditing Lights-Out Operations	304
Auditing Problem Management Operations	304
Auditing Monitoring Operations	305
Auditing Procurement	305
Questions	306
Answers	308
Chapter 6 Information Asset Protection	309
Information Security Management	309
Aspects of Information Security Management	309
Roles and Responsibilities	313

Asset Inventory and Classification	314
Access Controls	316
Privacy	318
Third-Party Management	319
Human Resources Security	323
Computer Crime	326
Security Incident Management	331
Forensic Investigations	334
Logical Access Controls	336
Access Control Concepts	336
Access Control Models	337
Threats	338
Vulnerabilities	339
Access Points and Methods of Entry	340
Identification, Authentication, and Authorization	343
Protecting Stored Information	351
Managing User Access	356
Protecting Mobile Devices	362
Network Security Controls	362
Network Security	362
Securing Client-Server Applications	365
Securing Wireless Networks	367
Protecting Internet Communications	370
Encryption	373
Voice over IP (VoIP)	385
Private Branch Exchange (PBX)	386
Malware	387
Information Leakage	392
Environmental Controls	393
Environmental Threats and Vulnerabilities	394
Environmental Controls and Countermeasures	395
Physical Security Controls	400
Physical Access Threats and Vulnerabilities	400
Physical Access Controls and Countermeasures	400
Auditing Asset Protection	401
Auditing Security Management	402
Auditing Logical Access Controls	403
Auditing Network Security Controls	410
Auditing Environmental Controls	413
Auditing Physical Security Controls	414
Chapter Notes	415
Summary	416
Questions	417
Answers	419

Chapter 7	Business Continuity and Disaster Recovery	421
	Disasters	422
	Types of Disasters	422
	How Disasters Affect Organizations	427
	The BCP Process	428
	BCP Policy	428
	Business Impact Analysis (BIA)	430
	Criticality Analysis	432
	Establishing Key Targets	434
	Developing Recovery Strategies	437
	Developing Recovery and Continuity Plans	447
	Considerations for Continuity and Recovery Plans	458
	Components of a Business Continuity Plan	463
	Testing Recovery Plans	464
	Testing Recovery and Continuity Plans	464
	Documenting Test Results	468
	Improving Recovery and Continuity Plans	469
	Training Personnel	469
	Making Plans Available to Personnel When Needed	470
	Maintaining Recovery and Continuity Plans	471
	Sources for Best Practices	471
	Auditing Business Continuity and Disaster Recovery	473
	Reviewing Business Continuity and Disaster Recovery Plans	474
	Reviewing Prior Test Results and Action Plans	476
	Evaluating Off-Site Storage	477
	Evaluating Alternative Processing Facilities	478
	Interviewing Key Personnel	478
	Reviewing Service Provider Contracts	479
	Reviewing Insurance Coverage	479
	Chapter Summary	480
	Chapter 7 Notes	481
	Questions	482
	Answers	484
Appendix A	Conducting a Professional Audit	485
	Introduction	485
	Understanding the Audit Cycle	485
	How the Information Systems Audit Cycle Is Discussed	486
	Use of the Word “Client” in This Appendix	486
	Overview of the IS Audit Cycle	487
	IS Audit Cycle at a High Level	487
	Project Origination	488
	Engagement Letters (“Contracts”) and Audit Charters	495
	Ethics and Independence	497

Launching a New Project: Planning an Audit	499
Understanding the Client's Needs	499
Performing a Risk Assessment	500
Audit Methodology	501
Developing the Audit Plan	503
Gathering Information—"PBC" Lists	503
A Client's Preparedness for an Audit	503
Developing Audit Objectives	504
Developing the Scope of an Audit	505
Developing a Testing Plan	506
Understand the Controls Environment	507
Perform a Pre-audit (or "Readiness Assessment")	515
Organize a Testing Plan	516
Resource Planning for the Audit Team	520
Project Execution	521
Project Planning with the Client	521
Gathering Testing Evidence	521
Launching Testing	523
Performing Tests of Control Existence	524
Perform Testing of Control Operating Effectiveness	526
Discovering Testing Exceptions	530
Discovering Incidents Requiring Immediate Attention	531
Materiality of Exceptions	533
Developing Audit Opinions	535
Developing Audit Recommendations	537
Managing Supporting Documentation	538
Delivering Final Reports	541
Writing the Report	541
Solicitation of Management's Response	542
Audit Closing Procedures	543
Audit Checklists	544
Delivery of the Report	544
Final Sign-off with the Client	544
Audit Follow-up	544
Retesting the Previous Period's Failed Controls	545
Follow-up on Management's Action Plans to Remediate	
Control Failures	545
Client Feedback and Evaluations	545
Appendix B Popular Methodologies, Frameworks, and Guidance	547
Common Terms and Concepts	547
Governance	548
Goals, Objectives, Strategies	548
Processes	549
Capability Maturity Models	550
Controls	550

	The Deming Cycle	553
	Projects	553
	Frameworks, Methodologies, and Guidance	554
	COSO Internal Control Integrated Framework	554
	COBIT	558
	GTAG	560
	GAIT	561
	ISF Standard of Good Practice	562
	ISO/IEC 27001 and 27002	562
	ITIL	564
	PMBOK	565
	PRINCE2	567
	Summary of Frameworks	568
	Pointers for Successful Use of Frameworks	568
	Summary	570
Appendix C	About the CD	571
	System Requirements	571
	Installing and Running MasterExam	571
	MasterExam	571
	Electronic Book	572
	Help	572
	Removing Installation(s)	572
	Technical Support	572
	LearnKey Technical Support	572
	Glossary	573
	Index	619

Figure Credits

Figure 5-2 courtesy of Fir0002/Flagstaffotos with permission granted under the terms of the GNU Free Documentation License, Version 1.2, http://commons.wikimedia.org/wiki/Commons:GNU_Free_Documentation_License_version_1.2.

Figure 5-3 courtesy of Sassospicco with permission granted under the terms of the Creative Commons Attribution Share-Alike 2.5 License, <http://creativecommons.org/licenses/by-sa/2.5/>.

Figure 5-4, courtesy of Rjt, has been released into the public domain by its author at the Polish Wikipedia project.

Figure 5-5 courtesy of Robert Kloosterhuis with permission granted under the terms of the Creative Commons Attribution Share-Alike 2.5 License, <http://creativecommons.org/licenses/by-sa/2.5/>.

Figure 5-13 courtesy of Rebecca Steele.

Figure 5-14 courtesy of Poil with permission granted under the terms of the GNU Free Documentation License, Version 1.2, http://commons.wikimedia.org/wiki/Commons:GNU_Free_Documentation_License,_version_1.2, and the Creative Commons Attribution ShareAlike 3.0 License, <http://creativecommons.org/licenses/by-sa/3.0/>.

Figure 5-15 courtesy of Hhedeshian with permission granted under the terms of the Creative Commons Attribution 3.0 Unported License, <http://creativecommons.org/licenses/by/3.0/>.

Figure 5-16 courtesy of FDominec with permission granted under the terms of the GNU Free Documentation License, Version 1.2, http://commons.wikimedia.org/wiki/Commons:GNU_Free_Documentation_License,_version_1.2.