

Contents

ABOUT THE EXAM.....	1
ABOUT THIS BOOK.....	2
HOW THE BOOK IS LAID OUT.....	2
HOW TO USE THIS BOOK.....	2
SECTION 1: THE PROCESS OF AUDITING INFORMATION SYSTEMS DOMAIN	3
CHAPTER 1: SOME ORGANIZATIONS, LAWS, STANDARDS AND FRAMEWORKS	4
ORGANIZATIONS	4
LAWS.....	4
STANDARDS	4
FRAMEWORKS	5
CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGIES, OR COBIT	11
TEST QUESTIONS.....	15
CHAPTER 2: ISAAS	17
STANDARDS	17
ISAAS GUIDELINES.....	20
TEST QUESTIONS.....	22
CHAPTER 3: FROM GOVERNANCE TO PROCEDURES.....	23
GOVERNANCE.....	23
GOAL.....	23
STRATEGY	23
POLICY	23
STANDARD.....	24
PROCEDURE	24
GUIDELINE	25
TOOLS AND TECHNOLOGIES.....	25
BRINGING IT ALL TOGETHER.....	25
TEST QUESTIONS.....	26
CHAPTER 4: KGI, CSF, KPI AND KRI	27
KGI	27
CSF	27
KPI	27
KRI	27
TEST QUESTIONS.....	28
CHAPTER 5: ALE, RTO, RPO, SDO, MTO, MTD AND AIW	29
ANNUAL LOSS EXPECTANCY, OR ALE.....	29
RECOVERY TIME OBJECTIVE, OR RTO.....	29
RECOVERY POINT OBJECTIVE, OR RPO	29
SERVICE DELIVERY OBJECTIVE, OR SDO	30

MAXIMUM TOLERABLE OUTAGE, OR MTO, OR MTD	30
ALLOWABLE INTERRUPTION WINDOW, OR AIW.....	30
BRINGING IT ALL TOGETHER.....	30
TEST QUESTIONS.....	32
CHAPTER 6: RISK APPETITE, TOLERANCE AND CAPACITY.....	33
OVERVIEW	33
TEST QUESTIONS.....	35
CHAPTER 7: FROM THREATS TO CONTROLS	36
RELATIONSHIPS.....	36
THREATS.....	36
INTERNAL THREATS.....	37
EXTERNAL THREATS	37
VULNERABILITIES.....	38
CONTROL STRENGTH.....	38
CONTROL TYPES.....	39
CONTROL CATEGORIES	39
CONTROL METHODS.....	40
INTERNAL CONTROLS	40
COUNTERMEASURES	41
TECHNICAL EXPOSURES	41
TEST QUESTIONS.....	42
CHAPTER 8: RISK MANAGEMENT	43
ISACA'S RISK IT FRAMEWORK	43
NIST SP 800-30.....	43
COBIT 5 RISK MANAGEMENT PROCESS	44
RISK ANALYSIS	45
EVALUATION OF RISK	46
CONFUSING TERMS	47
FRAUD	47
TEST QUESTIONS.....	49
CHAPTER 9: SAMPLING	50
STATISTICAL SAMPLING	50
NON-STATISTICAL SAMPLING.....	52
TEST QUESTIONS.....	54
CHAPTER 10: IS AUDITOR DUTIES FOR THE PROCESS OF AUDITING INFORMATION SYSTEM DOMAIN.....	55
MANAGEMENT OF THE IS AUDIT FUNCTION	55
ISACA IS AUDIT AND ASSURANCE STANDARDS AND GUIDELINES.....	56
PERFORMING AN IS AUDIT.....	57
COMMUNICATING AUDIT RESULTS	63
CONTROL SELF-ASSESSMENT	64
THE EVOLVING IS AUDIT PROCESS.....	65
TEST QUESTIONS.....	68

SECTION 2: THE GOVERNANCE AND MANAGEMENT OF IT DOMAIN	71
CHAPTER 11: SECURITY CONCEPTS.....	72
BASIC TERMS.....	72
SEGREGATION OF DUTY CONTROLS.....	73
PRIVACY	74
TEST QUESTIONS.....	75
CHAPTER 12: ROLES, RESPONSIBILITIES, AND A RACI MATRIX	76
OVERVIEW.....	76
TEST QUESTIONS.....	77
CHAPTER 13: HUMAN RESOURCES, OR HR.....	78
HIRING.....	78
EMPLOYEE HANDBOOK.....	78
TRAINING	78
EMPLOYEE PERFORMANCE	78
MANDATORY LEAVE AND JOB ROTATION	78
TERMINATION POLICIES	78
SECURITY AND THIRD PARTIES.....	79
TEST QUESTIONS.....	80
CHAPTER 14: OUTSOURCING	81
OUTSOURCING PRACTICES AND STRATEGIES	81
THIRD-PARTY REPORTS	83
OUTSOURCING GOVERNANCE	83
MANAGING THIRD-PARTY SERVICE DELIVERY	84
TEST QUESTIONS.....	85
CHAPTER 15: CLOUD COMPUTING	86
TYPES OF CLOUD COMPUTING	86
VIRTUALIZATION	88
WHY CLOUD COMPUTING HAS SUDDENLY APPEARED	88
RISKS AND CONTROLS	89
REWARDS VS. RISK	91
TEST QUESTIONS.....	92
CHAPTER 16: CAPITAL EXPENDITURES AND OPERATIONAL EXPENDITURES	93
OVERVIEW	93
TEST QUESTIONS.....	94
CHAPTER 17: BCP, DRP AND BIA	95
BUSINESS IMPACT ANALYSIS, OR BIA	96
BCP	97
OTHER PLANNING ISSUES.....	99
RECOVERY SITES.....	99
BASICS FOR RECOVERY SITE SELECTIONS	100

COMMUNICATION NETWORKS.....	100
HIGH-AVAILABILITY CONSIDERATIONS	101
BACKUP AND RESTORATION	102
TEST QUESTIONS.....	105
CHAPTER 18: PLAN TESTING.....	107
OVERVIEW.....	107
TEST QUESTIONS.....	109
CHAPTER 19: ENTERPRISE ARCHITECTURE	110
OVERVIEW.....	110
TEST QUESTIONS.....	111
CHAPTER 20: GOVERNANCE.....	112
CORPORATE GOVERNANCE.....	112
GOVERNANCE OF ENTERPRISE IT	112
TEST QUESTIONS.....	115
CHAPTER 21: INFORMATION SECURITY POLICY.....	116
OVERVIEW.....	116
TEST QUESTIONS.....	117
CHAPTER 22: INFORMATION TECHNOLOGY MANAGEMENT PRACTICES	118
FINANCIAL MANAGEMENT PRACTICES.....	118
QUALITY MANAGEMENT.....	118
INFORMATION SECURITY MANAGEMENT.....	118
PERFORMANCE OPTIMIZATION	118
TEST QUESTIONS.....	120
CHAPTER 23: IT ORGANIZATIONAL STRUCTURE ROLES AND RESPONSIBILITIES	121
OVERVIEW.....	121
TEST QUESTIONS.....	123
CHAPTER 24: IS AUDITOR DUTIES FOR THE GOVERNANCE AND MANAGEMENT OF IT DOMAIN	124
GEIT	124
INFORMATION SYSTEMS STRATEGY	124
MATURITY AND PROCESS IMPROVEMENT MODELS	125
IT INVESTMENT AND ALLOCATION PRACTICES	125
POLICIES AND PROCEDURES.....	125
OUTSOURCING	126
AUDITING IT GOVERNANCE STRUCTURE AND IMPLEMENTATION.....	126
AUDITING BUSINESS CONTINUITY	127
TEST QUESTIONS.....	129
SECTION 3: THE INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND IMPLEMENTATION DOMAIN	130
CHAPTER 25: PROJECT MANAGEMENT	131
STRUCTURE.....	131

PRACTICES	134
TEST QUESTIONS.....	140
CHAPTER 26: BENEFITS REALIZATION.....	142
MANAGING PORTFOLIOS, PROGRAMS AND PROJECTS	142
DEVELOPING THE BUSINESS CASE AND GETTING IT APPROVED.....	143
TECHNIQUES FOR BENEFITS REALIZATION.....	143
TEST QUESTIONS.....	144
CHAPTER 27: THE SOFTWARE DEVELOPMENT LIFE CYCLE, OR SDLC	145
BUSINESS APPLICATIONS.....	145
TRADITIONAL SDLC PHASES.....	147
STRUCTURED ANALYSIS, DESIGN AND DEVELOPMENT TECHNIQUES.....	155
AGILE DEVELOPMENT.....	155
SCRUM.....	155
PROTOTYPING DEVELOPMENT	157
RAPID APPLICATION DEVELOPMENT, OR RAD.....	157
OBJECT-ORIENTED SYSTEM DEVELOPMENT, OR OOSD	157
COMPONENT-BASED DEVELOPMENT.....	157
TEST QUESTIONS.....	158
CHAPTER 28: SOFTWARE DEVELOPMENT.....	160
ARCHITECTURE	160
OBJECT-ORIENTED PROGRAMMING, OR OOP	160
COMPONENT PROGRAMMING	161
WEB APPLICATIONS AND SERVICES	161
CASE TOOLS.....	162
FOURTH-GENERATION LANGUAGES, OR 4GLS	162
SOURCE CODE MANAGEMENT	163
TEST QUESTIONS.....	164
CHAPTER 29: E-COMMERCE	165
MODELS.....	165
BASIC REQUIREMENTS.....	165
RISK.....	165
TEST QUESTIONS.....	166
CHAPTER 30: EDI	167
TRADITIONAL EDI.....	167
WEB-BASED EDI	167
RISKS	168
CONTROLS	168
XML	168
CHAPTER 31: EMAIL	171
RISKS	171
CONTROLS	171

TEST QUESTIONS.....	173
CHAPTER 32: ELECTRIC MONEY.....	174
ELECTRONIC FUNDS TRANSFER, OR EFT.....	174
ELECTRONIC BANKING.....	174
POINT-OF-SALE SYSTEMS.....	174
AUTOMATED TELLER MACHINE, OR ATM	175
ELECTRONIC FINANCE.....	175
PAYMENT SYSTEMS	175
TEST QUESTIONS.....	177
CHAPTER 33: INTEGRATED MANUFACTURING SYSTEM, OR IMS	178
OVERVIEW.....	178
TEST QUESTIONS.....	179
CHAPTER 34: INDUSTRIAL CONTROL SYSTEMS, OR ICS.....	180
OVERVIEW.....	180
TEST QUESTIONS.....	181
CHAPTER 35: ARTIFICIAL INTELLIGENCE AND EXPERT SYSTEMS	182
OVERVIEW	182
TEST QUESTIONS.....	184
CHAPTER 36: BUSINESS INTELLIGENCE, OR BI	185
OVERVIEW.....	185
TEST QUESTIONS.....	188
CHAPTER 37: DECISION SUPPORT SYSTEM, OR DSS	189
OVERVIEW.....	189
TEST QUESTIONS.....	191
CHAPTER 38: RE-ENGINEERING	192
SOFTWARE REENGINEERING	192
BUSINESS PROCESS Re-ENGINEERING, OR BPR	192
TEST QUESTIONS.....	194
CHAPTER 39: OTHER BUSINESS APPLICATIONS	195
INTERACTIVE VOICE RESPONSE, OR IVR	195
PURCHASE ACCOUNTING SYSTEM.....	195
IMAGE PROCESSING	195
CUSTOMER RELATIONSHIP MANAGEMENT, OR CRM	195
SUPPLY CHAIN MANAGEMENT, OR SCM	196
TEST QUESTIONS.....	197
CHAPTER 40: INFRASTRUCTURE	198
OVERVIEW	198
TEST QUESTIONS.....	200

CHAPTER 41: MANAGING CHANGE, CONFIGURATION, PATCHES AND RELEASES	201
CONFIGURATION MANAGEMENT.....	202
PATCH MANAGEMENT	202
RELEASE MANAGEMENT.....	202
TEST QUESTIONS.....	204
CHAPTER 42: APPLICATION CONTROLS	205
INPUT CONTROLS	205
PROCESSING PROCEDURES	208
OUTPUT CONTROLS	210
TEST QUESTIONS.....	211
CHAPTER 43: IS AUDITOR DUTIES FOR THE INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND IMPLEMENTATION DOMAIN	212
PROJECT MANAGEMENT.....	212
BUSINESS APPLICATION DEVELOPMENT	212
SDLC.....	213
E-COMMERCE	213
EDI	214
POINT-OF-SALE	214
ELECTRONIC BANKING.....	214
INTEGRATED MANUFACTURING SYSTEMS, OR IMS	215
ATMs	215
AI AND EXPERT SYSTEMS	215
REVERSE ENGINEERING.....	216
INFRASTRUCTURE DEVELOPMENT AND ACQUISITION PRACTICES	216
HARDWARE ACQUISITION	217
CHANGE MANAGEMENT.....	217
SOFTWARE DEVELOPMENT.....	217
BUSINESS PROCESS ENGINEERING, OR BPR	218
AUDITING APPLICATION, PROCESSING AND OUTPUT CONTROLS	218
AUDITING SYSTEMS DEVELOPMENT, ACQUISITION AND MAINTENANCE	219
SOURCE CODE MANAGEMENT	221
TEST QUESTIONS.....	223
SECTION 4: THE INFORMATION SYSTEMS OPERATIONS, MAINTENANCE AND SERVICE MANAGEMENT DOMAIN	224
CHAPTER 44: INFORMATION SYSTEMS OPERATIONS	225
SLAs	225
JOB SCHEDULING.....	225
INCIDENT HANDLING.....	226
PROBLEM MANAGEMENT	226
ABNORMAL CONDITIONS	226
THE SUPPORT AND HELP DESK.....	226
IT ASSET MANAGEMENT	226

TEST QUESTIONS.....	227
CHAPTER 45: HARDWARE ARCHITECTURE	228
COMPUTER HARDWARE COMPONENTS AND ARCHITECTURE	228
HARDWARE MAINTENANCE PROGRAM.....	230
HARDWARE MONITORING PROCEDURES.....	231
CAPACITY MANAGEMENT	231
TEST QUESTIONS.....	232
CHAPTER 46: OPERATING SYSTEMS	233
OVERVIEW.....	233
TEST QUESTIONS.....	234
CHAPTER 47: DATABASE MANAGEMENT	235
QUALITY.....	235
THE DATA LIFE CYCLE.....	236
DATABASE MANAGEMENT SYSTEM, OR DBMS.....	236
DATABASE STRUCTURE	238
SECURING ACCESS	240
DATA COMMUNICATIONS SOFTWARE.....	240
TEST QUESTIONS.....	241
CHAPTER 48: THIRD-PARTY SOFTWARE	242
UTILITY PROGRAMS	242
SOFTWARE LICENSING.....	242
TEST QUESTIONS.....	243
CHAPTER 49: NETWORK INFRASTRUCTURE.....	244
CIRCUITS, SWITCHING AND BANDWIDTH.....	244
TYPES OF NETWORKS	245
NETWORK SERVICES	245
THE OSI ARCHITECTURE	246
TCP/IP MODEL.....	248
NETWORK PHYSICAL MEDIA.....	248
LAN TOPOLOGIES	249
MEDIA ACCESS TECHNOLOGIES.....	250
REPEATERS, HUBS, BRIDGES, SWITCHES AND ROUTERS.....	251
WAN TECHNOLOGIES	253
WIRELESS NETWORKS	256
NETWORK ACCESS FROM MOBILE DEVICES	257
HONEYPUOTS AND TARPITS.....	257
TEST QUESTIONS.....	258
CHAPTER 50: INTERNET CONCEPTS	261
DOMAIN NAME SERVICE AND URLs	261
WEB TECHNOLOGIES	261
TEST QUESTIONS.....	263

CHAPTER 51: TELECOMMUNICATIONS.....	264
PRIVATE BRANCH EXCHANGE, OR PBX	264
VOICE OVER IP, VoIP	267
TEST QUESTIONS.....	268
CHAPTER 52: IS AUDITOR DUTIES FOR THE INFORMATION SYSTEMS OPERATIONS, MAINTENANCE AND SERVICE MANAGEMENT DOMAIN	269
GENERAL AUDITING TIPS	269
AUDITING INFRASTRUCTURE AND OPERATIONS	269
TEST QUESTIONS.....	277
SECTION 5: THE PROTECTION OF INFORMATION ASSETS DOMAIN	278
CHAPTER 53: ASSET CLASSIFICATION	279
OVERVIEW	279
TEST QUESTIONS.....	280
CHAPTER 54: SECURITY AWARENESS AND TRAINING.....	281
OVERVIEW	281
TEST QUESTIONS.....	282
CHAPTER 55: EXTERNAL PARTIES	283
ADDRESSING SECURITY WHEN DEALING WITH CUSTOMERS	283
ADDRESSING SECURITY IN THIRD-PARTY AGREEMENTS	283
TEST QUESTIONS.....	285
CHAPTER 56: COMPUTER CRIME.....	286
TYPES OF DAMAGE	286
PERPETRATORS	286
CATEGORIES	287
ATTACKS.....	287
PLANNING FOR SECURITY INCIDENTS	291
INVESTIGATION OF COMPUTER CRIMES.....	292
TEST QUESTIONS.....	294
CHAPTER 57: LOGICAL ACCESS	297
PATHS.....	297
IDENTIFICATION	297
AUTHENTICATION.....	298
AUTHORIZATION	300
SSO	301
MANAGING LOGICAL ACCESS.....	301
AUDIT LOGGING.....	302
TEST QUESTIONS.....	304
CHAPTER 58: REMOTE CONNECTIVITY	305
OVERVIEW	305

TEST QUESTIONS.....	306
CHAPTER 59: MEDIA HANDLING	307
OVERVIEW.....	307
TEST QUESTIONS.....	308
CHAPTER 60: NETWORK SECURITY.....	309
LAN SECURITY.....	309
CLIENT-SERVER SECURITY	309
WIRELESS SECURITY THREATS AND RISK MITIGATION	309
INTERNET THREATS AND SECURITY.....	310
MOBILE COMPUTING	310
PEER-TO-PEER COMPUTING	312
INSTANT MESSAGING.....	312
SOCIAL MEDIA.....	312
END-USER COMPUTING	313
MANAGING THE NETWORK	313
TEST QUESTIONS.....	316
CHAPTER 61: FIREWALLS.....	317
PACKET FILTERING FIREWALLS	317
APPLICATION FIREWALLS	317
STATEFUL INSPECTION FIREWALLS	318
EXAMPLES OF FIREWALL IMPLEMENTATIONS.....	318
FIREWALL ISSUES.....	319
TEST QUESTIONS.....	320
CHAPTER 62: INTRUSION DETECTION	321
OVERVIEW.....	321
TEST QUESTIONS.....	323
CHAPTER 63: ENCRYPTION.....	324
KEY ELEMENTS OF ENCRYPTION SYSTEMS.....	324
HASHING	324
QUANTUM CRYPTOGRAPHY.....	325
SYMMETRIC VS. ASYMMETRIC.....	325
PUBLIC KEY SYSTEMS	325
APPLYING ENCRYPTION IN THE REAL WORLD	328
TEST QUESTIONS.....	329
CHAPTER 64: PENETRATION TESTING	330
AGREEMENT.....	330
TYPES OF PEN TESTING.....	330
PHASES	330
RISKS	331
TEST QUESTIONS.....	332

CHAPTER 65: ENVIRONMENTAL ISSUES	333
OVERVIEW.....	333
TEST QUESTIONS.....	336
CHAPTER 66: DATA LEAKAGE PREVENTION, OR DLP	337
OVERVIEW.....	337
TEST QUESTIONS.....	339
CHAPTER 67: PHYSICAL ACCESS	340
PHYSICAL ACCESS CONTROLS.....	340
TEST QUESTIONS.....	342
CHAPTER 68: IS AUDITOR DUTIES FOR THE PROTECTION OF INFORMATION ASSETS DOMAIN	343
CONTROL MONITORING AND EFFECTIVENESS.....	343
AUDITING SYSTEM ACCESS.....	343
PRIVACY PRINCIPLES AND THE ROLE OF THE AUDITOR.....	343
AUDITING COMPUTER CRIME	344
AUDITING NETWORK SECURITY.....	344
AUDITING PBX SYSTEMS	344
AUDITING THE INFORMATION SECURITY FRAMEWORK	345
AUDITING NETWORK INFRASTRUCTURE SECURITY.....	351
TEST QUESTIONS.....	355
TEST QUESTION ANSWERS.....	356
GLOSSARY.....	362
ACRONYMS.....	392
INDEX	397

Figures

Figure 1: Balanced Scorecard Dimensions	6
Figure 2: Characteristics of CMMI Maturity Levels	6
Figure 7: FEA Reference Models	7
Figure 8: ITIL Life Cycle.....	7
Figure 9: PDCA Methodology.....	9
Figure 10: TOGAF Architecture Development Cycle	10
Figure 11: The Zachman Framework	10
Figure 3: COBIT 5 Principles	11
Figure 4: COBIT 5 Enterprise Enablers	12
Figure 5: Overview of the Process Assessment Model	12
Figure 6: COBIT 5 Quality Subdimensions	13
Figure 12: ISAAS Standards and Guidelines	17
Figure 13: Goals, Strategies, Policies, Standards, Procedures and Guidelines.....	23
Figure 14: Optimizing Risk Costs	33
Figure 15: Information Security Relationships	36
Figure 16: Control Types and Effect	40
Figure 17: The Risk Management Process	43
Figure 18: Risk Assessment Process	44
Figure 19: Qualitative Impact Matrix	45
Figure 20: Semiquantitative Matrix	46
Figure 21: Risk Terms Demystified.....	47
Figure 22: Steps in the Selection of a Sample for an Audit Test	50
Figure 23: Precision vs. Accuracy	50
Figure 24: Sampling Methods	52
Figure 25: Audit Steps.....	58
Figure 26: Concurrent Audit Tools - Advantages and Disadvantages	67
Figure 27: Classic Architecture vs. Cloud Computing.....	86
Figure 28: Cloud Computing Deployment Models	87
Figure 29: 'as a Service' Offerings	87
Figure 30: Virtualization.....	88
Figure 31: Dynamically Spinning Up VMs As-Needed	89
Figure 32: Cloud Computing Risk Map.....	91
Figure 33:Techniques Implemented in Relation to RTOs and RPOs.....	102
Figure 34: Three Views of a Project	132
Figure 35: Resources and Duration Curve (TR)	135
Figure 36: The Five Steps of Project Management	135
Figure 37: Critical Path Example	137
Figure 38: Portfolios, Programs and Projects.....	142
Figure 39: The Traditional SDLC Approach.....	146
Figure 40: Primary and Foreign Keys	149
Figure 41: Scrum	156
Figure 42: Classes and Objects.....	161
Figure 43: EDI Example	167
Figure 44: An XML Example	169
Figure 45: An Expert System	182
Figure 46: BI Architecture	185
Figure 47: Application Control Categories	205
Figure 48: Application Input Controls	206
Figure 49: Application Processing Procedures	208
Figure 50: Application Output Controls	210
Figure 51: Basic Computer Components.....	228
Figure 52: Data Quality	235

Figure 53: The COBIT 5 Data Life Cycle	236
Figure 54: DBMS User Access	237
Figure 55: External Schema	237
Figure 56: Conceptual Schema	237
Figure 57: Internal Schema	238
Figure 58: Relational Database Example.....	239
Figure 59: The Result of a Join – a Conceptual View.....	239
Figure 60: Various Switching Technologies.....	244
Figure 61: Baseband vs. Broadband.....	245
Figure 62: Various Network Types	245
Figure 63: The OSI Model.....	246
Figure 64: OSI Layers and Typical Protocols.....	248
Figure 65: TCP/OSI Layer Mapping	248
Figure 66: A Ring Topology	249
Figure 67: A Bus Topology	249
Figure 68: A Star Topology.....	250
Figure 69: When to Use Each Network Device	253
Figure 70: Transmission Media Pros and Cons	253
Figure 71: CSU/DSU and DTE/DCE	254
Figure 72: Dual-Homed Firewall	318
Figure 73: Screened-Host Firewall	319
Figure 74: Screened-Subnet Firewall	319

Tables

Table 1: A RACI Example	76
Table 2: Basic Recovery Tests and Categories.....	107
Table 3: An ACL Example.....	300

About the Exam

The CISA exam is offered throughout the year, and there are no prerequisites required to take the exam. However, before the certification will be rewarded, you must have at least 5 years of experience in information system auditing, control or security. This experience must have occurred within the last 5 to 10 years.

For those not possessing the above requirements, there are several ways to fulfill the experience. For example, you may substitute 1 year of the 5 by working in information systems or in a non-IS auditing role. Another year can be filled if you have 60 hours of college credit or a qualifying degree. Unfortunately, you will always need at least 2 years of actual experience, possibly more.

The exam is a computer-based test available three times each year, 4-hours in length and consisting of 200 questions in a multiple-choice format. While ISACA does not advertise the percentage of questions you must correctly answer in order to pass, a decent estimate is between 50%-60%. This is based wholly on anecdotal evidence and may be inaccurate. But, we do know that the pass rate is around 50% - roughly half of all candidates will fail the test the first time. Successful candidates can work towards the experience requirements and apply for the certificate.

As of the print date for this book, the cost for ISACA members is \$575 and \$760 for non-members.