

CISSP[®] STUDY GUIDE

Eric Conrad ■ Seth Misenar ■ Joshua Feldman

- Pass the exam the first time
- Filled with real-world examples, questions, and answers
- Companion Web site contains two full-length practice exams to help you prepare for test day

Contents

Acknowledgments	xvii
About the authors	xix

CHAPTER 1	Introduction	1
	How to Prepare for the Exam	2
	The Notes Card Approach	2
	Practice Tests	2
	Read the Glossary	3
	Readiness Checklist	3
	How to Take the Exam	3
	Steps to Becoming a CISSP®	3
	Exam Logistics	4
	How to Take the Exam	5
	After the Exam	6
	Good Luck!	6

CHAPTER 2	Domain 1: Information security governance and risk management	7
	Unique Terms and Definitions	7
	Introduction	7
	Cornerstone Information Security Concepts	8
	Confidentiality, Integrity, and Availability	8
	Identity and Authentication, Authorization, and Accountability	10
	Risk Analysis	13
	Assets	13
	Threats and Vulnerabilities	13
	Risk = Threat × Vulnerability	14
	Impact	15
	Risk Analysis Matrix	15
	Calculating Annualized Loss Expectancy	16
	Total Cost of Ownership	17
	Return on Investment	18
	Risk Choices	19
	Qualitative and Quantitative Risk Analysis	20
	The Risk Management Process	21
	Information Security Governance	22

Security Policy and Related Documents	22
Security Awareness and Training	24
Roles and Responsibilities	25
Compliance with Laws and Regulations	26
Privacy	26
Due Care and Due Diligence	26
Best Practice	27
Outsourcing and Offshoring.....	27
Auditing and Control Frameworks	28
Certification and Accreditation.....	30
Ethics	31
The (ISC) ² © Code of Ethics	31
Summary of Exam Objectives	32
Self Test.....	32
Self Test Quick Answer Key	34

CHAPTER 3	Domain 2: Access control.....	37
	Unique Terms and Definitions.....	37
	Introduction.....	37
	Cornerstone Access Control Concepts	38
	The CIA triad	38
	Identification and AAA.....	40
	Subjects and objects	41
	Access Control Models	41
	Discretionary Access Controls (DAC).....	42
	Mandatory Access Controls (MAC)	42
	Non-Discretionary Access Control	42
	Content and Context-Dependent Access Controls	44
	Centralized Access Control.....	44
	Decentralized Access Control	44
	Access Control Protocols and Frameworks.....	45
	Procedural Issues for Access Control.....	47
	Labels, Clearance, Formal Access Approval, and Need to Know	48
	Rule-Based Access Controls	50
	Access Control Lists	50
	Access Control Defensive Categories and Types	50
	Preventive	51
	Detective	51
	Corrective.....	51
	Recovery	52

Deterrent	52
Compensating	52
Comparing Access Controls.....	52
Authentication Methods	53
Type 1 Authentication: Something You Know.....	53
Type 2 Authentication: Something You Have	59
Type 3 Authentication: Something You Are	61
Someplace You Are	67
Access Control Technologies.....	67
Single Sign-On (SSO)	67
Kerberos	68
SESAME.....	72
Security Audit Logs	72
Types of Attackers	73
Hackers	73
Black Hats and White Hats.....	74
Script Kiddies	74
Outsiders	75
Insiders.....	76
Hacktivist.....	77
Bots and BotNets.....	77
Phishers and Spear Phishers.....	79
Assessing Access Control	79
Penetration Testing.....	82
Vulnerability Testing.....	84
Security Audits	84
Security Assessments	84
Summary of Exam Objectives	85
Self Test.....	85
Self Test Quick Answer Key	88

CHAPTER 4 Domain 3: Cryptography	91
Unique Terms and Definitions.....	91
Introduction.....	91
Cornerstone Cryptographic Concepts	91
Key Terms	92
Confidentiality, Integrity, Authentication, and Non-Repudiation.....	92
Confusion, Diffusion, Substitution, and Permutation	92
Cryptographic Strength	93
Monoalphabetic and Polyalphabetic Ciphers	93

Modular Math.....	93
Exclusive Or (XOR).....	93
Types of Cryptography	95
History of Cryptography	95
Egyptian Hieroglyphics.....	95
Spartan Scytale	96
Caesar Cipher and other Rotation Ciphers.....	96
Vigenère Cipher.....	97
Cipher Disk.....	97
Jefferson Disks	98
Book Cipher and Running-Key Cipher	100
Codebooks.....	100
One-Time Pad.....	100
Hebern Machines and Purple	102
Cryptography Laws	105
Symmetric Encryption.....	105
Stream and Block Ciphers	106
Initialization Vectors and Chaining	106
Data Encryption Standard	106
International Data Encryption Algorithm (IDEA)	110
Advanced Encryption Standard (AES)	110
Blowfish and Twofish	113
RC5 and RC6	113
Asymmetric Encryption.....	113
Asymmetric Methods	114
Hash Functions	116
Collisions	116
MD5	116
Secure Hash Algorithm	116
HAVAL.....	117
Cryptographic Attacks.....	117
Brute Force	117
Known Plaintext	117
Chosen Plaintext and Adaptive Chosen Plaintext.....	118
Chosen Ciphertext and Adaptive Chosen Ciphertext.....	118
Meet-in-the-middle Attack	118
Known Key.....	119
Differential Cryptanalysis	119
Linear Cryptanalysis.....	119
Side-channel Attacks	119

Birthday Attack	119
Key Clustering.....	120
Implementing Cryptography	120
Digital Signatures	120
HMAC.....	121
CBC-MAC	122
Public Key Infrastructure	122
IPsec.....	122
SSL and TLS	124
PGP	124
S/MIME	125
Escrowed Encryption.....	125
Steganography	125
Digital Watermarks	126
Summary of Exam Objectives	127
Self Test.....	127
Self Test Quick Answer Key.....	129

CHAPTER 5	Domain 4: Physical (Environmental) security.....	131
	Unique Terms and Definitions.....	131
	Introduction.....	131
	Perimeter Defenses	132
	Fences	132
	Gates	132
	Bollards	132
	Lights	133
	CCTV.....	133
	Locks.....	135
	Smart Cards and Magnetic Stripe Cards	138
	Tailgating/piggybacking	138
	Mantraps and Turnstiles	140
	Contraband Checks.....	140
	Motion Detectors and Other Perimeter Alarms	140
	Doors and Windows	141
	Walls, floors, and ceilings.....	142
	Guards	142
	Dogs	143
	Restricted Areas and Escorts	143
	Site Selection, Design, and Configuration	144
	Site Selection Issues	144
	Site Design and Configuration Issues.....	144

System Defenses.....	146
Asset Tracking.....	146
Port Controls.....	146
Drive and Tape Encryption.....	146
Media Storage and Transportation.....	147
Media Cleaning and Destruction	147
Environmental Controls.....	149
Electricity.....	149
HVAC	151
Heat, Flame, and Smoke Detectors	152
Safety Training and Awareness	153
ABCD Fires and Suppression	154
Types of Fire Suppression Agents.....	156
Summary of Exam Objectives	160
Self Test.....	160
Self Test Quick Answer Key	163

CHAPTER 6	Domain 5: Security architecture and design	165
	Unique Terms and Definitions.....	165
	Introduction.....	165
	Secure System Design Concepts.....	166
	Layering	166
	Abstraction.....	166
	Security Domains	167
	The Ring Model	167
	Open and Closed Systems.....	168
	Secure Hardware Architecture.....	168
	The System Unit and Motherboard	168
	The Computer Bus	169
	The CPU	170
	Memory.....	172
	Memory Protection.....	174
	Secure Operating System and Software Architecture.....	177
	The Kernel.....	178
	Users and File Permissions	178
	Virtualization	181
	Thin Clients	182
	System Vulnerabilities, Threats, and Countermeasures	183
	Emanations.....	183
	Covert Channels	183
	Buffer Overflows.....	184

TOCTOU/Race Conditions	185
Backdoors	185
Malicious Code (Malware)	186
Server-Side Attacks	187
Client-Side Attacks.....	188
Web Application Attacks	189
Mobile Device Attacks.....	190
Database Security	191
Countermeasures.....	193
Security Models.....	193
Reading Down and Writing Up.....	193
State Machine model.....	195
Bell-LaPadula model.....	195
Lattice-Based Access Controls	196
Integrity Models	197
Information Flow Model.....	198
Chinese Wall Model.....	199
Noninterference	199
Take-Grant	199
Access Control Matrix	200
Zachman Framework for Enterprise Architecture.....	200
Graham-Denning Model.....	200
Harrison-Ruzzo-Ullman Model.....	201
Modes of Operation.....	202
Evaluation Methods, Certification, and Accreditation.....	202
The Orange Book	203
ITSEC	204
The International Common Criteria.....	205
PCI-DSS.....	206
Certification and Accreditation.....	206
Summary of Exam Objectives	206
Self Test.....	207
Self Test Quick Answer Key	209

CHAPTER 7

Domain 6: Business continuity and disaster recovery planning	211
Unique Terms and Definitions.....	211
Introduction.....	211
BCP and DRP Overview and Process	212
Business Continuity Planning (BCP).....	212
Disaster Recovery Planning (DRP)	213

Relationship between BCP and DRP	213
Disasters or disruptive Events.....	214
The Disaster Recovery Process.....	221
Developing a BCP/DRP	223
Project Initiation	224
Scoping the Project	227
Assessing the Critical State.....	227
Conduct Business Impact Analysis (BIA).....	228
Identify Preventive Controls	232
Recovery Strategy	232
Related Plans	236
Plan Approval	241
Backups and Availability	241
Hardcopy Data.....	242
Electronic Backups.....	243
Software Escrow.....	245
DRP Testing, Training, and Awareness	245
DRP Testing	246
Training.....	248
Awareness.....	248
Continued BCP/DRP Maintenance	248
Change Management	248
BCP/DRP Mistakes	249
Specific BCP/DRP Frameworks	249
NIST SP 800-34	249
ISO/IEC-27031	250
BS-25999	250
BCI.....	251
Summary of Exam Objectives	251
Self Test.....	251
Self Test Quick Answer Key	253

CHAPTER 8	Domain 7: Telecommunications and network security	255
	Unique Terms and Definitions.....	255
	Introduction.....	255
	Network Architecture and Design	256
	Network Defense-in-Depth	256
	Fundamental Network Concepts	256
	The OSI Model.....	259
	The TCP/IP Model	261
	Encapsulation.....	262

Network Access, Internet and Transport Layer Protocols and Concepts	263
Application Layer TCP/IP Protocols and Concepts.....	276
Layer 1 Network Cabling	281
LAN Technologies and Protocols.....	283
LAN Physical Network Topologies.....	285
WAN Technologies and Protocols	288
Network Devices and Protocols.....	291
Repeater and Hubs	291
Bridges	292
Switches	293
TAPs	294
Routers	295
Firewalls.....	299
Modem	306
DTE/DCE and CSU/DSU	306
Intrusion Detection Systems and Intrusion Prevention Systems	306
Honeypots	309
Network Attacks	310
Network Scanning Tools.....	311
Secure Communications.....	312
Authentication Protocols and Frameworks.....	312
VPN.....	314
VoIP	316
Wireless Local Area Networks	317
RFID	321
Remote Access	322
Summary of Exam Objectives	324
Self Test.....	325
Self Test Quick Answer Key	327

CHAPTER 9	Domain 8: Application development security	329
	Unique Terms and Definitions.....	329
	Introduction.....	329
	Programming Concepts	330
	Machine Code, Source Code, and Assemblers	330
	Compilers, Interpreters, and Bytecode	330
	Procedural and Object-Oriented Languages.....	331
	Fourth-generation Programming Language	333
	Computer-Aided Software Engineering (CASE)	333

Top-Down versus Bottom-Up Programming.....	333
Types of Publicly Released Software.....	334
Application Development Methods	335
Waterfall Model.....	336
Sashimi Model.....	337
Agile Software Development.....	339
Spiral	340
Rapid Application Development (RAD)	341
Prototyping.....	341
SDLC	342
Software Escrow.....	346
Object-Orientated Design and Programming	346
Object-Oriented Programming (OOP)	346
Object Request Brokers.....	349
Object-Oriented Analysis (OOA) and Object-Oriented Design (OOD).....	351
Software Vulnerabilities, Testing, and Assurance	351
Software Vulnerabilities.....	352
Software Testing Methods	353
Disclosure	355
Software Capability Maturity Model (CMM).....	356
Databases	356
Types of Databases	357
Database Integrity.....	361
Database Replication and Shadowing.....	361
Data Warehousing and Data Mining	362
Artificial Intelligence	362
Expert Systems	362
Artificial Neural Networks.....	363
Bayesian Filtering.....	364
Genetic Algorithms and Programming	365
Summary of Exam Objectives	365
Self Test.....	366
Self Test Quick Answer Key	368

CHAPTER 10 Domain 9: Operations security	371
Unique Terms and Definitions.....	371
Introduction.....	371
Administrative Security.....	372
Administrative Personnel Controls	372
Privilege Monitoring	375

Sensitive Information/Media Security	376
Sensitive Information	376
Asset Management	378
Configuration Management.....	379
Change Management.....	381
Continuity of Operations.....	383
Service Level Agreements (SLA).....	383
Fault Tolerance.....	384
Incident Response Management	390
Methodology	391
Types of attacks.....	393
Summary of Exam Objectives	398
Self Test.....	400
Self Test Quick Answer Key.....	403

CHAPTER 11 Domain 10: Legal regulations, investigations, and

compliance.....	405
Unique Terms and Definitions.....	405
Introduction.....	406
Major Legal Systems.....	406
Civil Law (legal system).....	406
Common Law	406
Religious Law.....	407
Other Systems.....	407
Criminal, Civil, and Administrative Law.....	407
Criminal Law	408
Civil Law	408
Administrative Law	409
Information Security Aspects of Law.....	409
Computer Crime	410
Intellectual Property	411
Import/export Restrictions.....	415
Privacy	416
Liability.....	419
Legal Aspects of Investigations.....	420
Digital Forensics.....	420
Incident Response.....	423
Evidence.....	423
Evidence Integrity	425
Chain of Custody.....	426

Reasonable Searches	426
Entrapment and enticement.....	428
Important Laws and Regulations	429
U.S. Computer Fraud and Abuse Act.....	430
USA PATRIOT Act	431
HIPAA	431
United States Breach Notification Laws	432
Ethics	433
Computer Ethics Institute.....	433
IAB's Ethics and the Internet	434
The (ISC) ² © Code of Ethics	434
Summary of Exam Objectives	435
Self Test.....	436
Self Test Quick Answer Key	438

Appendix: Self test.....	441
Glossary	489
Index.....	525