

CISSP®: **Certified Information Systems Security Professional**

Study Guide

3rd Edition



James Michael Stewart

Ed Tittel

Mike Chapple

San Francisco • London



Contents

<i>Introduction</i>		<i>xxiii</i>
<i>Assessment Test</i>		<i>xxxi</i>
Chapter 1	Accountability and Access Control	1
	Access Control Overview	2
	Types of Access Control	2
	Access Control in a Layered Environment	5
	The Process of Accountability	5
	Identification and Authentication Techniques	9
	Passwords	10
	Biometrics	13
	Tokens	18
	Tickets	20
	Single Sign On	20
	Access Control Techniques	23
	Discretionary Access Controls (DAC)	23
	Nondiscretionary Access Controls	24
	Mandatory Access Controls	24
	Role-Based Access Control (RBAC)	25
	Lattice-Based Access Controls	26
	Access Control Methodologies and Implementation	27
	Centralized and Decentralized Access Control	27
	RADIUS and TACACS	27
	Access Control Administration	28
	Account Administration	29
	Account, Log, and Journal Monitoring	30
	Access Rights and Permissions	30
	Summary	32
	Exam Essentials	34
	Review Questions	36
	Answers to Review Questions	40
Chapter 2	Attacks and Monitoring	43
	Monitoring	44
	Intrusion Detection	45
	Host-Based and Network-Based IDSs	46
	Knowledge-Based and Behavior-Based Detection	47
	IDS-Related Tools	48
	Penetration Testing	49

	Methods of Attacks	50
	Brute Force and Dictionary Attacks	51
	Denial of Service	52
	Spoofing Attacks	55
	Man-in-the-Middle Attacks	56
	Sniffer Attacks	57
	Spamming Attacks	57
	Crackers	58
	Access Control Compensations	58
	Summary	59
	Exam Essentials	59
	Review Questions	62
	Answers to Review Questions	66
Chapter 3	ISO Model, Network Security, and Protocols	69
	OSI Model	70
	History of the OSI Model	70
	OSI Functionality	71
	Encapsulation/Deencapsulation	72
	OSI Layers	73
	TCP/IP Model	78
	Communications and Network Security	79
	Network Cabling	79
	LAN Technologies	84
	Network Topologies	87
	TCP/IP Overview	89
	Internet/Intranet/Extranet Components	96
	Firewalls	97
	Other Network Devices	100
	Remote Access Security Management	102
	Network and Protocol Security Mechanisms	103
	VPN Protocols	103
	Secure Communications Protocols	104
	E-Mail Security Solutions	105
	Dial-Up Protocols	105
	Authentication Protocols	106
	Centralized Remote Authentication Services	106
	Network and Protocol Services	107
	Frame Relay	107
	Other WAN Technologies	108
	Avoiding Single Points of Failure	108
	Redundant Servers	109
	Failover Solutions	109
	RAID	110

	Summary	111
	Exam Essentials	112
	Review Questions	114
	Answers to Review Questions	118
Chapter 4	Communications Security and Countermeasures	121
	Virtual Private Network (VPN)	122
	Tunneling	123
	How VPNs Work	124
	Implementing VPNs	124
	Network Address Translation	125
	Private IP Addresses	125
	Stateful NAT	126
	Switching Technologies	126
	Circuit Switching	126
	Packet Switching	127
	Virtual Circuits	127
	WAN Technologies	128
	WAN Connection Technologies	129
	Encapsulation Protocols	130
	Miscellaneous Security Control Characteristics	131
	Transparency	131
	Verifying Integrity	131
	Transmission Mechanisms	132
	Managing E-Mail Security	132
	E-Mail Security Goals	132
	Understanding E-Mail Security Issues	133
	E-Mail Security Solutions	134
	Securing Voice Communications	136
	Social Engineering	136
	Fraud and Abuse	137
	Phreaking	138
	Security Boundaries	139
	Network Attacks and Countermeasures	139
	Eavesdropping	140
	Second-Tier Attacks	140
	Address Resolution Protocol (ARP)	141
	Summary	142
	Exam Essentials	143
	Review Questions	146
	Answers to Review Questions	150
Chapter 5	Security Management Concepts and Principles	153
	Security Management Concepts and Principles	154
	Confidentiality	154

	Integrity	155
	Availability	156
	Other Security Concepts	157
	Protection Mechanisms	159
	Layering	160
	Abstraction	160
	Data Hiding	160
	Encryption	161
	Change Control/Management	161
	Data Classification	162
	Summary	165
	Exam Essentials	166
	Review Questions	168
	Answers to Review Questions	172
Chapter 6	Asset Value, Policies, and Roles	175
	Employment Policies and Practices	176
	Security Management for Employees	176
	Security Roles	179
	Security Management Planning	181
	Policies, Standards, Baselines, Guidelines, and Procedures	182
	Security Policies	182
	Security Standards, Baselines, and Guidelines	184
	Security Procedures	184
	Risk Management	185
	Risk Terminology	186
	Risk Assessment Methodologies	188
	Quantitative Risk Analysis	190
	Qualitative Risk Analysis	193
	Handling Risk	195
	Security Awareness Training	196
	Summary	197
	Exam Essentials	199
	Review Questions	202
	Answers to Review Questions	206
Chapter 7	Data and Application Security Issues	209
	Application Issues	210
	Local/Nondistributed Environment	210
	Distributed Environment	212
	Databases and Data Warehousing	216
	Database Management System (DBMS) Architecture	216
	Database Transactions	219

Security for Multilevel Databases	220
ODBC	222
Aggregation	223
Data Mining	224
Data/Information Storage	225
Types of Storage	225
Storage Threats	226
Knowledge-Based Systems	226
Expert Systems	227
Neural Networks	228
Decision Support Systems	228
Security Applications	229
Systems Development Controls	229
Software Development	229
Systems Development Life Cycle	234
Life Cycle Models	237
Gantt Charts and PERT	240
Change Control and Configuration Management	242
Software Testing	243
Security Control Architecture	244
Service Level Agreements	247
Summary	247
Exam Essentials	248
Written Lab	249
Review Questions	250
Answers to Review Questions	254
Answers to Written Lab	256

Chapter 8 Malicious Code and Application Attacks 257

Malicious Code	258
Sources	258
Viruses	259
Logic Bombs	264
Trojan Horses	264
Worms	265
Active Content	267
Countermeasures	267
Password Attacks	268
Password Guessing	269
Dictionary Attacks	269
Social Engineering	270
Countermeasures	270
Denial of Service Attacks	271
SYN Flood	271

	Distributed DoS Toolkits	272
	Smurf	273
	Teardrop	274
	Land	276
	DNS Poisoning	276
	Ping of Death	276
	Application Attacks	277
	Buffer Overflows	277
	Time-of-Check-to-Time-of-Use	278
	Trap Doors	278
	Rootkits	278
	Reconnaissance Attacks	278
	IP Probes	279
	Port Scans	279
	Vulnerability Scans	279
	Dumpster Diving	280
	Masquerading Attacks	280
	IP Spoofing	280
	Session Hijacking	281
	Decoy Techniques	281
	Honey Pots	281
	Pseudo-Flaws	281
	Summary	282
	Exam Essentials	283
	Written Lab	284
	Review Questions	285
	Answers to Review Questions	289
	Answers to Written Lab	291
Chapter 9	Cryptography and Private Key Algorithms	293
	History	294
	Caesar Cipher	294
	American Civil War	295
	Ultra vs. Enigma	295
	Cryptographic Basics	296
	Goals of Cryptography	296
	Cryptography Concepts	297
	Cryptographic Mathematics	299
	Ciphers	305
	Modern Cryptography	310
	Cryptographic Keys	311
	Symmetric Key Algorithms	312
	Asymmetric Key Algorithms	313
	Hashing Algorithms	316

- 27.** B. Layers 1 and 2 contain device drivers but are not normally implemented in practice. Layer 0 always contains the security kernel. Layer 3 contains user applications. Layer 4 does not exist. For more information, please see Chapter 7.
- 28.** C. Transposition ciphers use an encryption algorithm to rearrange the letters of the plaintext message to form a ciphertext message. For more information, please see Chapter 9.
- 29.** C. The annualized loss expectancy (ALE) is computed as the product of the asset value (AV) times the annualized rate of occurrence (ARO). The other formulas displayed here do not accurately reflect this calculation. For more information, please see Chapter 15.
- 30.** C. The principle of integrity states that objects retain their veracity and are only intentionally modified by authorized subjects. For more information, please see Chapter 5.
- 31.** D. E-mail is the most common delivery mechanism for viruses, worms, Trojan horses, documents with destructive macros, and other malicious code. For more information, please see Chapter 4.
- 32.** A. Technical security controls include access controls, intrusion detection, alarms, CCTV, monitoring, HVAC, power supplies, and fire detection and suppression. For more information, please see Chapter 19.
- 33.** A. Administrative determinations of federal agencies are published as the Code of Federal Regulations. For more information, please see Chapter 17.
- 34.** A. Identification of priorities is the first step of the Business Impact Assessment process. For more information, please see Chapter 15.
- 35.** C. Any recipient can use Mike's public key to verify the authenticity of the digital signature. For more information, please see Chapter 10.
- 36.** C. A Type 3 authentication factor is something you are, such as fingerprints, voice print, retina pattern, iris pattern, face shape, palm topology, hand geometry, and so on. For more information, please see Chapter 1.
- 37.** C. The primary goal of risk management is to reduce risk to an acceptable level. For more information, please see Chapter 6.

	Symmetric Cryptography	316
	Data Encryption Standard (DES)	316
	Triple DES (3DES)	318
	International Data Encryption Algorithm (IDEA)	319
	Blowfish	319
	Skipjack	320
	Advanced Encryption Standard (AES)	320
	Key Distribution	322
	Key Escrow	324
	Summary	324
	Exam Essentials	325
	Written Lab	327
	Review Questions	328
	Answers to Review Questions	332
	Answers to Written Lab	334
Chapter 10	PKI and Cryptographic Applications	335
	Asymmetric Cryptography	336
	Public and Private Keys	337
	RSA	337
	El Gamal	338
	Elliptic Curve	339
	Hash Functions	340
	SHA	341
	MD2	342
	MD4	342
	MD5	343
	Digital Signatures	344
	HMAC	345
	Digital Signature Standard	345
	Public Key Infrastructure	346
	Certificates	346
	Certificate Authorities	347
	Certificate Generation and Destruction	348
	Key Management	350
	Applied Cryptography	350
	Electronic Mail	351
	Web	353
	E-Commerce	354
	Networking	355
	Cryptographic Attacks	359
	Summary	360
	Exam Essentials	361
	Review Questions	363
	Answers to Review Questions	367

Chapter 11	Principles of Computer Design	369
	Computer Architecture	371
	Hardware	371
	Input/Output Structures	389
	Firmware	391
	Security Protection Mechanisms	391
	Technical Mechanisms	391
	Security Policy and Computer Architecture	393
	Policy Mechanisms	394
	Distributed Architecture	395
	Security Models	397
	State Machine Model	397
	Information Flow Model	398
	Noninterference Model	398
	Take-Grant Model	398
	Access Control Matrix	399
	Bell-LaPadula Model	400
	Biba	402
	Clark-Wilson	403
	Brewer and Nash Model (a.k.a. Chinese Wall)	403
	Classifying and Comparing Models	404
	Summary	405
	Exam Essentials	406
	Review Questions	408
	Answers to Review Questions	412
Chapter 12	Principles of Security Models	415
	Common Security Models, Architectures, and Evaluation Criteria	416
	Trusted Computing Base (TCB)	417
	Security Models	418
	Objects and Subjects	420
	Closed and Open Systems	421
	Techniques for Ensuring Confidentiality, Integrity, and Availability	422
	Controls	423
	Trust and Assurance	423
	Understanding System Security Evaluation	424
	Rainbow Series	424
	ITSEC Classes and Required Assurance and Functionality	428
	Common Criteria	429
	Certification and Accreditation	432
	Common Flaws and Security Issues	435
	Covert Channels	435

	Attacks Based on Design or Coding Flaws and Security Issues	435
	Programming	439
	Timing, State Changes, and Communication Disconnects	439
	Electromagnetic Radiation	439
	Summary	440
	Exam Essentials	441
	Review Questions	443
	Answers to Review Questions	447
Chapter 13	Administrative Management	449
	Operations Security Concepts	450
	Antivirus Management	451
	Operational Assurance and Life Cycle Assurance	452
	Backup Maintenance	452
	Changes in Workstation/Location	453
	Need-to-Know and the Principle of Least Privilege	453
	Privileged Operations Functions	454
	Trusted Recovery	455
	Configuration and Change Management Control	455
	Standards of Due Care and Due Diligence	456
	Privacy and Protection	457
	Legal Requirements	457
	Illegal Activities	457
	Record Retention	458
	Sensitive Information and Media	458
	Security Control Types	461
	Operations Controls	462
	Personnel Controls	464
	Summary	466
	Exam Essentials	467
	Review Questions	470
	Answers to Review Questions	474
Chapter 14	Auditing and Monitoring	477
	Auditing	478
	Auditing Basics	478
	Audit Trails	480
	Reporting Concepts	481
	Sampling	482
	Record Retention	483
	External Auditors	484
	Monitoring	484
	Monitoring Tools and Techniques	485

Penetration Testing Techniques	486
Planning Penetration Testing	487
Penetration Testing Teams	488
Ethical Hacking	488
War Dialing	488
Sniffing and Eavesdropping	489
Radiation Monitoring	490
Dumpster Diving	490
Social Engineering	491
Problem Management	491
Inappropriate Activities	491
Indistinct Threats and Countermeasures	492
Errors and Omissions	492
Fraud and Theft	493
Collusion	493
Sabotage	493
Loss of Physical and Infrastructure Support	493
Malicious Hackers or Crackers	495
Espionage	495
Malicious Code	495
Traffic and Trend Analysis	495
Initial Program Load Vulnerabilities	496
Summary	497
Exam Essentials	498
Review Questions	502
Answers to Review Questions	506
Chapter 15	Business Continuity Planning
	509
Business Continuity Planning	510
Project Scope and Planning	511
Business Organization Analysis	511
BCP Team Selection	512
Resource Requirements	513
Legal and Regulatory Requirements	514
Business Impact Assessment	515
Identify Priorities	516
Risk Identification	516
Likelihood Assessment	517
Impact Assessment	518
Resource Prioritization	519
Continuity Strategy	519
Strategy Development	519
Provisions and Processes	520
Plan Approval	522

Plan Implementation	522
Training and Education	522
BCP Documentation	523
Continuity Planning Goals	523
Statement of Importance	523
Statement of Priorities	524
Statement of Organizational Responsibility	524
Statement of Urgency and Timing	524
Risk Assessment	524
Risk Acceptance/Mitigation	525
Vital Records Program	525
Emergency Response Guidelines	525
Maintenance	525
Testing	526
Summary	526
Exam Essentials	526
Review Questions	528
Answers to Review Questions	532
Chapter 16	Disaster Recovery Planning
	535
Disaster Recovery Planning	536
Natural Disasters	537
Man-Made Disasters	541
Recovery Strategy	545
Business Unit Priorities	545
Crisis Management	546
Emergency Communications	546
Work Group Recovery	546
Alternate Processing Sites	547
Mutual Assistance Agreements	550
Database Recovery	551
Recovery Plan Development	552
Emergency Response	553
Personnel Notification	553
Backups and Offsite Storage	554
Software Escrow Arrangements	557
External Communications	558
Utilities	558
Logistics and Supplies	558
Recovery vs. Restoration	558
Training and Documentation	559
Testing and Maintenance	560
Checklist Test	560
Structured Walk-Through	560

	Simulation Test	561
	Parallel Test	561
	Full-Interruption Test	561
	Maintenance	561
	Summary	561
	Exam Essentials	562
	Written Lab	563
	Review Questions	564
	Answers to Review Questions	568
	Answers to Written Lab	570
Chapter 17	Law and Investigations	571
	Categories of Laws	572
	Criminal Law	572
	Civil Law	573
	Administrative Law	574
	Laws	574
	Computer Crime	575
	Intellectual Property	578
	Licensing	584
	Import/Export	584
	Privacy	585
	Investigations	590
	Evidence	591
	Investigation Process	593
	Summary	595
	Exam Essentials	595
	Written Lab	597
	Review Questions	598
	Answers to Review Questions	602
	Answers to Written Lab	604
Chapter 18	Incidents and Ethics	605
	Major Categories of Computer Crime	606
	Military and Intelligence Attacks	607
	Business Attacks	607
	Financial Attacks	608
	Terrorist Attacks	608
	Grudge Attacks	609
	“Fun” Attacks	609
	Evidence	610
	Incident Handling	610
	Common Types of Incidents	611

	Response Teams	612
	Abnormal and Suspicious Activity	614
	Confiscating Equipment, Software, and Data	614
	Incident Data Integrity and Retention	615
	Reporting Incidents	615
	Ethics	616
	(ISC) ² Code of Ethics	616
	Ethics and the Internet	617
	Summary	618
	Exam Essentials	619
	Review Questions	621
	Answers to Review Questions	625
Chapter 19	Physical Security Requirements	627
	Facility Requirements	628
	Secure Facility Plan	629
	Physical Security Controls	629
	Site Selection	629
	Visibility	630
	Accessibility	630
	Natural Disasters	630
	Facility Design	630
	Work Areas	630
	Server Rooms	631
	Visitors	631
	Forms of Physical Access Controls	631
	Fences, Gates, Turnstiles, and Mantraps	632
	Lighting	633
	Security Guards and Dogs	634
	Keys and Combination Locks	634
	Badges	635
	Motion Detectors	635
	Intrusion Alarms	635
	Secondary Verification Mechanisms	636
	Technical Controls	636
	Smart Cards	637
	Proximity Readers	637
	Access Abuses	638
	Intrusion Detection Systems	638
	Emanation Security	639
	Environment and Life Safety	640
	Personnel Safety	640
	Power and Electricity	640
	Noise	642

Temperature, Humidity, and Static	642
Water	643
Fire Detection and Suppression	643
Equipment Failure	647
Summary	648
Exam Essentials	649
Review Questions	652
Answers to Review Questions	656
Glossary	659
<i>Index</i>	725