

CISSP[®]

Certified Information Systems Security Professional

Study Guide

Fifth Edition



James Michael Stewart

Ed Tittel

Mike Chapple



WILEY

Wiley Publishing, Inc.

Acknowledgments

I hope our efforts to improve this study guide will lend themselves handily to your understanding and comprehension of the wide berth of CISSP concepts. I'd like to express my thanks to Sybex for continuing to support this project. Thanks to Ed Tittel and Mike Chapple for continuing to contribute to this project. Also thanks to all my CISSP course students who have provided their insight and input to improve my training courseware and ultimately this tome. Extra thanks to the 5th Edition Technical Editor, Darril Gibson, who performed amazing feats in guiding us to improve this book.

To my wonderful wife, Cathy, our life together is just getting started. To my son, Xzavier Slayde, and daughter, Remington Annaliese, may you grow to be more than we could imagine. To my parents, Dave and Sue, thanks for your love and consistent support. To Mark, as best friends go, it could've been worse. And finally, as always, to Elvis—all hail the King!

—*James Michael Stewart*

Thanks to both Michael Stewart and Mike Chapple for continuing to keep me involved in this project. Michael continues to teach CISSP courses with amazing frequency, which provides us with a lifeline to the hard-working professionals in the trenches for whom this credential means so much. Congrats again to Michael on another addition to his family; my son, Gregory, is now in first grade and the time just keeps flying by. May the months and years slip by as pleasantly and painlessly for you as they have for us. Next, thanks to the folks at Sybex, especially Jeff Kellum for rounding us all up and keeping us headed in the same direction and for his excellent view of where we need to take this book. Finally, I'd like to thank my loving and lovely wife, Dina, for all the great things she does to make family life so comfortable, clean, interesting and fun.

—*Ed Tittel*

Special thanks go to the information security team at the University of Notre Dame. Gary Dobbins, Bob Winding, David Seidl, and Robert Riley provided hours of interesting conversation and debate on security issues that inspired and informed much of the material in this book.

I would like to thank the team at Wiley who provided invaluable assistance throughout the book development process. I also owe a debt of gratitude to my literary agent, Carole Jelen of Waterside Productions. My coauthors, Ed Tittel and James Michael Stewart, have worked with me ever since we published the first edition of this book together eight years ago. I'd also like to thank the many people who participated in the production of this book but whom I never had the chance to meet: the graphics team, the production staff, and all of those involved in bringing this book to press.

—*Mike Chapple*

About the Authors

James Michael Stewart, CISSP, has been writing and training for more than 16 years, with a current focus on security. He has been teaching CISSP training courses since 2002, not to mention other courses on Windows security and ethical hacking/penetration testing. He is the author of several books and courseware sets on security certification, Microsoft topics, and network administration. More information about Michael can be found at his website: www.impactonline.com.

Ed Tittel is a full-time freelance writer, trainer, and consultant specializing in matters related to information security, markup languages, and networking technologies. He is a regular contributor to numerous TechTarget websites (and keeps updating his security certification survey for SearchSecurity.com), teaches online security and technology courses for HP, and enjoys his occasional gigs as an expert witness on Web technologies from the mid-1990s when he was lucky enough to write a raft of books in that arena. Ed's professional bio and other information are available at www.edtittel.com.

Mike Chapple, CISSP, PhD, is an IT professional with the University of Notre Dame. In the past, he was chief information officer of Brand Institute and an information security researcher with the National Security Agency and the U.S. Air Force. His primary areas of expertise include network intrusion detection and access controls. Mike is a frequent contributor to TechTarget's SearchSecurity site and the author of several information security titles including *The GSEC Prep Guide* from Wiley and *Information Security Illuminated* from Jones and Bartlett Publishers.

Contents at a Glance

<i>Introduction</i>		<i>xxix</i>
Chapter 1	Accountability and Access Control	1
Chapter 2	Attacks and Monitoring	49
Chapter 3	ISO Model, Protocols, Network Security, and Network Infrastructure	83
Chapter 4	Communications Security and Countermeasures	153
Chapter 5	Security Management Concepts and Principles	197
Chapter 6	Asset Value, Policies, and Roles	223
Chapter 7	Data and Application Security Issues	265
Chapter 8	Malicious Code and Application Attacks	321
Chapter 9	Cryptography and Symmetric Key Algorithms	365
Chapter 10	PKI and Cryptographic Applications	409
Chapter 11	Principles of Computer Design	447
Chapter 12	Principles of Security Models	489
Chapter 13	Administrative Management	537
Chapter 14	Auditing and Monitoring	571
Chapter 15	Business Continuity Planning	611
Chapter 16	Disaster Recovery Planning	641
Chapter 17	Law and Investigations	681
Chapter 18	Incidents and Ethics	717
Chapter 19	Physical Security Requirements	747
Appendix	About the Companion CD	785
<i>Index</i>		789

Contents

Introduction

xxix

Chapter 1	Accountability and Access Control	1
	Access Control Overview	2
	Types of Access Control	3
	Access Control in a Layered Environment	5
	The Process of Accountability	6
	Identification and Authentication Techniques	10
	Passwords	11
	Biometrics	14
	Tokens	19
	Tickets	21
	Single Sign-On	21
	Access Control Techniques	24
	Discretionary Access Controls	25
	Nondiscretionary Access Controls	25
	Mandatory Access Controls	26
	Role-Based Access Control	27
	Lattice-Based Access Controls	28
	Access Control Methodologies and Implementation	29
	Centralized and Decentralized Access Control	29
	RADIUS and TACACS	30
	Access Control Administration	31
	Account Administration	31
	Account, Log, and Journal Monitoring	32
	Access Rights and Permissions	33
	Summary	37
	Exam Essentials	38
	Written Lab	40
	Answers to Written Lab	41
	Review Questions	42
	Answers to Review Questions	46
Chapter 2	Attacks and Monitoring	49
	Monitoring	50
	Intrusion Detection	52
	Host- and Network-Based IDSs	54
	Knowledge- and Behavior-Based Detection	56
	IDS-Related Tools	57
	Understanding Honeypots	58

	Understanding Padded Cells	58
	Understanding Vulnerability Scanners	59
	Penetration Testing	59
	Methods of Attack	60
	Brute-Force and Dictionary Attacks	61
	Denial-of-Service Attacks	64
	Spoofing Attacks	68
	Man-in-the-Middle Attacks	69
	Sniffer Attacks	70
	Spamming Attacks	70
	Crackers, Hackers, and Attackers	71
	Access Control Compensations	71
	Summary	72
	Exam Essentials	73
	Written Lab	75
	Answers to Written Lab	76
	Review Questions	77
	Answers to Review Questions	81
Chapter 3	ISO Model, Protocols, Network Security, and Network Infrastructure	83
	OSI Model	84
	History of the OSI Model	85
	OSI Functionality	85
	Encapsulation/Deencapsulation	86
	OSI Layers	88
	TCP/IP Model	94
	Communications and Network Security	95
	Network Cabling	96
	LAN Technologies	109
	Network Topologies	113
	TCP/IP Overview	116
	Internet/Intranet/Extranet Components	127
	Firewalls	128
	Other Network Devices	132
	Remote Access Security Management	135
	Network and Protocol Security Mechanisms	137
	Secure Communications Protocols	137
	Dial-Up Protocols	138
	Authentication Protocols	139
	Centralized Remote Authentication Services	139
	Avoiding Single Points of Failure	140
	Redundant Servers	140

	Failover Solutions	140
	RAID	141
	Summary	142
	Exam Essentials	143
	Written Lab	145
	Answers to Written Lab	146
	Review Questions	147
	Answers to Review Questions	151
Chapter 4	Communications Security and Countermeasures	153
	Virtual Private Network (VPN)	154
	Tunneling	155
	How VPNs Work	156
	Implementing VPNs	157
	Network Address Translation	158
	Private IP Addresses	160
	Stateful NAT	161
	Static and Dynamic NAT	161
	Automatic Private IP Addressing (APIPA)	162
	Switching Technologies	163
	Circuit Switching	163
	Packet Switching	164
	Virtual Circuits	164
	WAN Technologies	165
	WAN Connection Technologies	167
	Dial-Up Encapsulation Protocols	169
	Miscellaneous Security Control Characteristics	170
	Transparency	170
	Verifying Integrity	170
	Transmission Mechanisms	171
	Managing Email Security	172
	Email Security Goals	172
	Understanding Email Security Issues	173
	Email Security Solutions	174
	Securing Voice Communications	176
	Social Engineering	177
	Fraud and Abuse	178
	Phreaking	179
	Security Boundaries	180
	Network Attacks and Countermeasures	181
	Eavesdropping	181
	Impersonation/Masquerading	183
	Replay Attacks	183

	Modification Attacks	183
	Address Resolution Protocol Spoofing	183
	DNS Poisoning, Spoofing, and Hijacking	184
	Hyperlink Spoofing	184
	Summary	185
	Exam Essentials	187
	Written Lab	189
	Answers to Written Lab	190
	Review Questions	191
	Answers to Review Questions	195
Chapter 5	Security Management Concepts and Principles	197
	Security Management Concepts and Principles	198
	Confidentiality	199
	Integrity	199
	Availability	201
	Standards of Due Care and Due Diligence	202
	Other Security Concepts	202
	Protection Mechanisms	206
	Layering	206
	Abstraction	207
	Data Hiding	207
	Encryption	207
	Change Control/Management	208
	Data Classification	209
	Planning to Plan	212
	Summary	213
	Exam Essentials	214
	Written Lab	215
	Answers to Written Lab	216
	Review Questions	217
	Answers to Review Questions	221
Chapter 6	Asset Value, Policies, and Roles	223
	Employment Policies and Practices	225
	Security Roles	231
	Security Management Planning	232
	Policies, Standards, Baselines, Guidelines, and Procedures	234
	Security Policies	234
	Security Standards, Baselines, and Guidelines	236
	Security Procedures	236
	Risk Management	237
	Risk Terminology	238

	Risk Assessment Methodologies	240
	Quantitative Risk Analysis	243
	Qualitative Risk Analysis	248
	Handling Risk	250
	Security Awareness Training	252
	Summary	253
	Exam Essentials	254
	Written Lab	257
	Answers to Written Lab	258
	Review Questions	259
	Answers to Review Questions	263
Chapter 7	Data and Application Security Issues	265
	Application Issues	266
	Local/Nondistributed Environment	266
	Distributed Environment	268
	Databases and Data Warehousing	273
	Database Management System (DBMS)	
	Architecture	273
	Database Transactions	277
	Security for Multilevel Databases	279
	ODBC	281
	Aggregation	282
	Data Mining	283
	Data/Information Storage	285
	Types of Storage	285
	Storage Threats	286
	Knowledge-Based Systems	286
	Expert Systems	286
	Neural Networks	288
	Decision Support Systems	288
	Security Applications	289
	Systems Development Controls	289
	Software Development	289
	Systems Development Life Cycle	295
	Life Cycle Models	298
	Gantt Charts and PERT	304
	Change Control and Configuration Management	305
	Software Testing	306
	Security Control Architecture	307
	Service-Level Agreements	310
	Summary	311
	Exam Essentials	311

	Written Lab	313
	Answers to Written Lab	314
	Review Questions	315
	Answers to Review Questions	319
Chapter 8	Malicious Code and Application Attacks	321
	Malicious Code	322
	Sources	322
	Viruses	323
	Logic Bombs	329
	Trojan Horses	329
	Worms	330
	Spyware and Adware	332
	Active Content	332
	Countermeasures	333
	Password Attacks	334
	Password Guessing	335
	Dictionary Attacks	336
	Social Engineering	336
	Countermeasures	337
	Denial-of-Service Attacks	338
	SYN Flood	338
	Distributed DoS Toolkits	339
	Smurf	340
	DNS Amplification Attacks	341
	Teardrop	342
	Land	343
	DNS Poisoning	343
	Ping of Death	344
	Application Attacks	345
	Buffer Overflows	345
	Time-of-Check-to-Time-of-Use	346
	Trap Doors	346
	Rootkits	346
	Web Application Security	346
	Cross-Site Scripting (XSS)	347
	SQL Injection	347
	Reconnaissance Attacks	350
	IP Probes	350
	Port Scans	351
	Vulnerability Scans	351
	Dumpster Diving	352
	Masquerading Attacks	352

	IP Spoofing	352
	Session Hijacking	353
	Decoy Techniques	353
	Honeypots	353
	Pseudoflaws	354
	Summary	354
	Exam Essentials	355
	Written Lab	356
	Answers to Written Lab	357
	Review Questions	358
	Answers to Review Questions	362
Chapter 9	Cryptography and Symmetric Key Algorithms	365
	Historical Milestones in Cryptography	366
	Caesar Cipher	366
	American Civil War	367
	Ultra vs. Enigma	368
	Cryptographic Basics	368
	Goals of Cryptography	368
	Cryptography Concepts	370
	Cryptographic Mathematics	371
	Ciphers	377
	Modern Cryptography	384
	Cryptographic Keys	384
	Symmetric Key Algorithms	385
	Asymmetric Key Algorithms	386
	Hashing Algorithms	389
	Symmetric Cryptography	390
	Data Encryption Standard	390
	Triple DES	392
	International Data Encryption Algorithm	393
	Blowfish	393
	Skipjack	394
	Advanced Encryption Standard	394
	Key Distribution	396
	Key Escrow	398
	Summary	398
	Exam Essentials	399
	Written Lab	401
	Answers to Written Lab	402
	Review Questions	403
	Answers to Review Questions	407

Chapter 10	PKI and Cryptographic Applications	409
	Asymmetric Cryptography	410
	Public and Private Keys	410
	RSA	411
	El Gamal	413
	Elliptic Curve	413
	Hash Functions	414
	SHA	415
	MD2	416
	MD4	416
	MD5	417
	Digital Signatures	418
	HMAC	419
	Digital Signature Standard	420
	Public Key Infrastructure	420
	Certificates	420
	Certificate Authorities	421
	Certificate Generation and Destruction	422
	Key Management	424
	Applied Cryptography	425
	Portable Devices	425
	Electronic Mail	426
	Web	428
	E-commerce	429
	Networking	430
	Cryptographic Attacks	434
	Summary	436
	Exam Essentials	437
	Written Lab	438
	Answers to Written Lab	439
	Review Questions	440
	Answers to Review Questions	444
Chapter 11	Principles of Computer Design	447
	Computer Architecture	449
	Hardware	449
	Input/Output Structures	469
	Firmware	470
	Security Protection Mechanisms	472
	Technical Mechanisms	472
	Security Policy and Computer Architecture	475
	Policy Mechanisms	475
	Distributed Architecture	477

	Summary	479
	Exam Essentials	480
	Written Lab	481
	Answers to Written Lab	482
	Review Questions	483
	Answers to Review Questions	487
Chapter 12	Principles of Security Models	489
	Security Models	491
	Trusted Computing Base (TCB)	492
	State Machine Model	493
	Information Flow Model	494
	Noninterference Model	494
	Take-Grant Model	495
	Access Control Matrix	495
	Bell-LaPadula Model	496
	Biba Model	498
	Clark-Wilson Model	500
	Brewer and Nash Model (aka Chinese Wall)	501
	Objects and Subjects	501
	Closed and Open Systems	502
	Techniques for Ensuring Confidentiality, Integrity, and Availability	503
	Controls	504
	Trust and Assurance	505
	Understanding System Security Evaluation	505
	Rainbow Series	506
	ITSEC Classes and Required Assurance and Functionality	511
	Common Criteria	512
	Industry and International Security Implementation Guidelines	515
	Certification and Accreditation	516
	Common Flaws and Security Issues	519
	Covert Channels	519
	Attacks Based on Design or Coding Flaws and Security Issues	520
	Programming	523
	Timing, State Changes, and Communication Disconnects	524
	Technology and Process Integration	524
	Electromagnetic Radiation	525
	Summary	525
	Exam Essentials	526

	Written Lab	528
	Answers to Written Lab	529
	Review Questions	530
	Answers to Review Questions	534
Chapter 13	Administrative Management	537
	Operations Security Concepts	538
	Antivirus Management	539
	Operational Assurance and Life Cycle Assurance	540
	Backup Maintenance	541
	Changes in Workstation/Location	542
	Need to Know and the Principle of Least Privilege	543
	Privileged Operations Functions	544
	Trusted Recovery	545
	Configuration and Change Management Control	546
	Standards of Due Care and Due Diligence	548
	Privacy and Protection	548
	Legal Requirements	549
	Illegal Activities	549
	Record Retention	549
	Sensitive Information and Media	550
	Security Control Types	553
	Operations Controls	554
	Personnel Controls	557
	Summary	558
	Exam Essentials	560
	Written Lab	562
	Answers to Written Lab	563
	Review Questions	564
	Answers to Review Questions	568
Chapter 14	Auditing and Monitoring	571
	Auditing	572
	Auditing Basics	572
	Audit Trails	574
	Reporting Concepts	576
	Sampling	577
	Record Retention	578
	External Auditors	579
	Monitoring	579
	Monitoring Tools and Techniques	580
	Warning Banners	580
	Keystroke Monitoring	580

Traffic Analysis and Trend Analysis	581
Other Monitoring Tools	581
Penetration-Testing Techniques	582
Planning Penetration Testing	583
Penetration Testing Teams	584
Ethical Hacking	586
War Dialing	586
Sniffing and Eavesdropping	587
Radiation Monitoring	587
Dumpster Diving	588
Social Engineering	589
Problem Management	590
Inappropriate Activities	590
Indistinct Threats and Countermeasures	591
Errors and Omissions	592
Fraud and Theft	592
Collusion	593
Sabotage	593
Loss of Physical and Infrastructure Support	594
Malicious Attackers	595
Espionage	595
Malicious Code	596
Traffic and Trend Analysis	597
Initial Program Load Vulnerabilities	597
Summary	598
Exam Essentials	599
Written Lab	602
Answers to Written Lab	603
Review Questions	604
Answers to Review Questions	608
Chapter 15 Business Continuity Planning	611
Business Continuity Planning	612
Project Scope and Planning	613
Business Organization Analysis	614
BCP Team Selection	614
Resource Requirements	616
Legal and Regulatory Requirements	618
Business Impact Assessment	619
Identify Priorities	620
Risk Identification	620
Likelihood Assessment	621
Impact Assessment	622
Resource Prioritization	624

Continuity Planning	624
Strategy Development	625
Provisions and Processes	625
Plan Approval	627
Plan Implementation	627
Training and Education	627
BCP Documentation	628
Continuity Planning Goals	628
Statement of Importance	628
Statement of Priorities	629
Statement of Organizational Responsibility	629
Statement of Urgency and Timing	629
Risk Assessment	629
Risk Acceptance/Mitigation	630
Vital Records Program	630
Emergency-Response Guidelines	630
Maintenance	630
Testing	631
Summary	631
Exam Essentials	632
Written Lab	633
Answers to Written Lab	634
Review Questions	635
Answers to Review Questions	639
Chapter 16 Disaster Recovery Planning	641
The Nature of Disaster	642
Natural Disasters	643
Man-Made Disasters	648
Recovery Strategy	652
Business Unit and Functional Priorities	653
Crisis Management	654
Emergency Communications	654
Work Group Recovery	655
Alternate Processing Sites	655
Mutual Assistance Agreements	659
Database Recovery	660
Recovery Plan Development	661
Emergency Response	662
Personnel Notification	663
Backups and Offsite Storage	664
Software Escrow Arrangements	667
External Communications	668

	Utilities	668
	Logistics and Supplies	668
	Recovery vs. Restoration	668
	Training and Documentation	669
	Testing and Maintenance	670
	Checklist Test	670
	Structured Walk-Through	671
	Simulation Test	671
	Parallel Test	671
	Full-Interruption Test	671
	Maintenance	672
	Summary	672
	Exam Essentials	673
	Written Lab	673
	Answers to Written Lab	674
	Review Questions	675
	Answers to Review Questions	679
Chapter 17	Law and Investigations	681
	Categories of Laws	682
	Criminal Law	682
	Civil Law	684
	Administrative Law	684
	Laws	685
	Computer Crime	685
	Intellectual Property	689
	Licensing	695
	Import/Export	695
	Privacy	696
	Investigations	702
	Evidence	703
	Investigation Process	705
	Summary	707
	Exam Essentials	708
	Written Lab	709
	Answers to Written Lab	710
	Review Questions	711
	Answers to Review Questions	715
Chapter 18	Incidents and Ethics	717
	Major Categories of Computer Crime	718
	Military and Intelligence Attacks	719
	Business Attacks	719

Financial Attacks	720
Terrorist Attacks	720
Grudge Attacks	721
Thrill Attacks	722
Evidence	723
Incident Handling	724
Common Types of Incidents	724
Response Teams	726
Incident Response Process	728
Interviewing Individuals	731
Incident Data Integrity and Retention	731
Reporting Incidents	732
Ethics	733
(ISC) ² Code of Ethics	734
Ethics and the Internet	735
Summary	736
Exam Essentials	736
Written Lab	738
Answers to Written Lab	739
Review Questions	740
Answers to Review Questions	744
Chapter 19	Physical Security Requirements
	747
Facility Requirements	749
Secure Facility Plan	749
Physical Security Controls	749
Site Selection	751
Visibility	751
Accessibility and Perimeter Security	751
Natural Disasters	752
Facility Design	752
Work Areas	752
Server Rooms	753
Visitors	754
Forms of Physical Access Controls	755
Fences, Gates, Turnstiles, and Mantraps	755
Lighting	756
Security Guards and Dogs	757
Keys and Combination Locks	758
Badges	759
Motion Detectors	759
Intrusion Alarms	760
Secondary Verification Mechanisms	760

Technical Controls	761	
Smart Cards	761	
Proximity Readers	762	
Access Abuses	762	
Intrusion Detection Systems	763	
Emanation Security	764	
Environment and Life Safety	765	
Personnel Safety	765	
Power and Electricity	766	
Noise	767	
Temperature, Humidity, and Static	767	
Water	768	
Fire Detection and Suppression	768	
Equipment Failure	773	
Summary	774	
Exam Essentials	775	
Written Lab	777	
Answers to Written Lab	778	
Review Questions	779	
Answers to Review Questions	783	
Appendix	About the Companion CD	785
<i>Index</i>		789