(ISC)²®

CISSP®

Certified Information Systems Security Professional

Official Study Guide

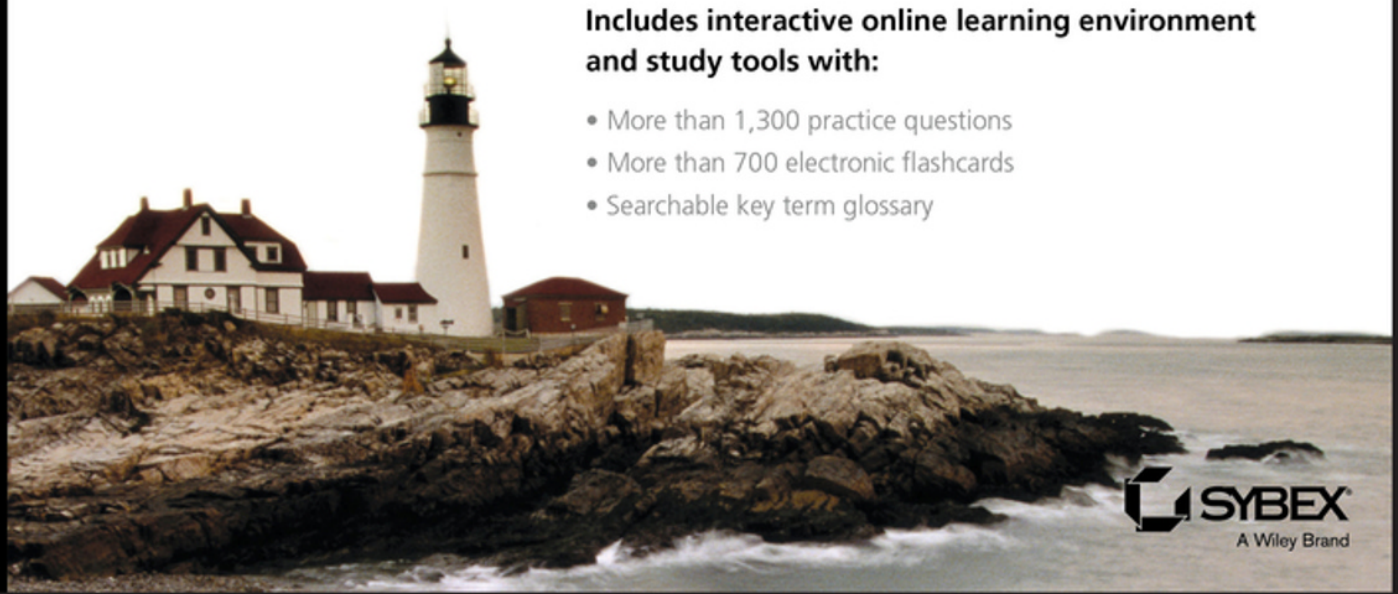
Eighth Edition

Mike Chapple, CISSP
James Michael Stewart, CISSP
Darril Gibson, CISSP

Covers all of the 2018 updated exam objectives, including Asset Security, Software Development Security, Security Operations, and much more...

Includes interactive online learning environment and study tools with:

- More than 1,300 practice questions
- More than 700 electronic flashcards
- Searchable key term glossary



SYBEX
A Wiley Brand

(ISC)²

CISSP®

Official Study Guide

Eighth Edition

(ISC)²

CISSP® Certified Information Systems Security Professional

Official Study Guide

Eighth Edition

Mike Chapple

James Michael Stewart

Darril Gibson

SYBEX®
A Wiley Brand

Development Editor: Kelly Talbot
Technical Editors: Jeff Parker, Bob Sipes, and David Seidl
Copy Editor: Kim Wimpsett
Editorial Manager: Pete Gaughan
Production Manager: Kathleen Wisor
Executive Editor: Jim Minatel
Proofreader: Amy Schneider
Indexer: Johnna VanHoose Dinse
Project Coordinator, Cover: Brent Savage
Cover Designer: Wiley
Cover Image: ©Getty Images Inc./Jeremy Woodhouse

Published simultaneously in Canada

ISBN: 978-1-119-47593-4
ISBN: 978-1-119-47595-8 (ebk.)
ISBN: 978-1-119-47587-3 (ebk.)

Manufactured in the United States of America

Library of Congress Control Number: 2018933561

10 9 8 7 6 5 4 3 2 1

To Dewitt Latimer, my mentor, friend, and colleague. I miss you dearly.
—Mike Chapple

To Cathy, your perspective on the world and life often surprises me, challenges me, and makes me love you even more.
—James Michael Stewart

To Nimfa, thanks for sharing your life with me for the past 26 years and letting me share mine with you.
—Darril Gibson

Dear Future (ISC)² Member,

Congratulations on starting your journey to CISSP® certification. Earning your CISSP is an exciting and rewarding milestone in your cybersecurity career. Not only does it demonstrate your ability to develop and manage nearly all aspects of an organization's cybersecurity operations, but you also signal to employers your commitment to life-long learning and taking an active role in fulfilling the (ISC)² vision of inspiring a safe and secure cyber world.

The material in this study guide is based upon the (ISC)² CISSP Common Body of Knowledge. It will help you prepare for the exam that will assess your competency in the following eight domains:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

While this study guide will help you prepare, passing the CISSP exam depends on your mastery of the domains combined with your ability to apply those concepts using your real-world experience.

I wish you the best of luck as you continue on your path to become a CISSP and certified member of (ISC)².

Sincerely,

David Shearer, CISSP
CEO
(ISC)²

Acknowledgments

We'd like to express our thanks to Sybex for continuing to support this project. Extra thanks to the eighth edition developmental editor, Kelly Talbot, and technical editors, Jeff Parker, Bob Sipes, and David Seidl, who performed amazing feats in guiding us to improve this book. Thanks as well to our agent, Carole Jelen, for continuing to assist in nailing down these projects.

—Mike, James, and Darril

Special thanks go to the information security team at the University of Notre Dame, who 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, James Michael Stewart and Darril Gibson, were great collaborators. Jeff Parker, Bob Sipes, and David Seidl, our diligent and knowledgeable technical editors, provided valuable in-sight as we brought this edition to press.

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

Thanks to Mike Chapple and Darril Gibson for continuing to contribute to this project. Thanks also to all my CISSP course students who have provided their insight and input to improve my training courseware and ultimately this tome. To my adoring wife, Cathy: Building a life and a family together has been more wonderful than I could have ever imagined. To Slayde and Remi: You are growing up so fast and learning at an outstanding pace, and you continue to delight and impress me daily. You are both growing into amazing individuals. To my mom, Johnnie: It is wonderful to have you close by. To Mark: No matter how much time has passed or how little we see each other, I have been and always will be your friend. And finally, as always, to Elvis: You were way ahead of the current bacon obsession with your peanut butter/banana/bacon sandwich; I think that's proof you traveled through time!

—James Michael Stewart

Thanks to Jim Minatel and Carole Jelen for helping get this update in place before $(ISC)^2$ released the objectives. This helped us get a head start on this new edition, and we appreciate your efforts. It's been a pleasure working with talented people like James Michael Stewart and Mike Chapple. Thanks to both of you for all your work and collaborative efforts on this project. The technical editors, Jeff Parker, Bob Sipes, and David Seidl, provided us with some outstanding feedback, and this book is better because of their efforts. Thanks to the team at Sybex (including project managers, editors, and graphics artists) for all the work you did helping us get this book to print. Last, thanks to my wife, Nimfa, for putting up with my odd hours as I worked on this book.

—Darril Gibson

About the Authors

Mike Chapple, CISSP, PhD, Security+, CISA, CySA+, is an associate teaching professor of IT, analytics, and operations at 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 more than 25 books including the companion book to this study guide: *CISSP Official (ISC)² Practice Tests*, the *CompTIA CSA+ Study Guide*, and *Cyberwarfare: Information Operations in a Connected World*. Mike offers study groups for the CISSP, SSCP, Security+, and CSA+ certifications on his website at `www.certmike.com`.

James Michael Stewart, CISSP, CEH, ECSA, CHFI, Security+, Network+, has been writing and training for more than 20 years, with a current focus on security. He has been teaching CISSP training courses since 2002, not to mention other courses on Internet security and ethical hacking/penetration testing. He is the author of and contributor to more than 75 books and numerous courseware sets on security certification, Microsoft topics, and network administration, including the *Security+ (SY0-501) Review Guide*. More information about Michael can be found at his website at `www.impactonline.com`.

Darril Gibson, CISSP, Security+, CASP, is the CEO of YCDA (short for You Can Do Anything), and he has authored or coauthored more than 40 books. Darril regularly writes, consults, and teaches on a wide variety of technical and security topics and holds several certifications. He regularly posts blog articles at `http://blogs.getcertifiedgetahead.com/` about certification topics and uses that site to help people stay abreast of changes in certification exams. He loves hearing from readers, especially when they pass an exam after using one of his books, and you can contact him through the blogging site.

About the Technical Editors

Jeff T. Parker, CISSP, is a technical editor and reviewer across many focuses of information security. Jeff regularly contributes to books, adding experience and practical know-how where needed. Jeff's experience comes from 10 years of consulting with Hewlett-Packard in Boston and from 4 years with Deutsche-Post in Prague, Czech Republic. Now residing in Canada, Jeff teaches his and other middle-school kids about building (and destroying) a home lab. He recently coauthored *Wireshark for Security Professionals* and is now authoring *CySA+ Practice Exams*. Keep learning!

Bob Sipes, CISSP, is an enterprise security architect and account security officer at DXC Technology providing tactical and strategic leadership for DXC clients. He holds several certifications, is actively involved in security organizations including ISSA and Infragard, and is an experienced public speaker on topics including cybersecurity, communications, and leadership. In his spare time, Bob is an avid antiquarian book collector with an extensive library of 19th and early 20th century boys' literature. You can follow Bob on Twitter at `@bobsipes`.

David Seidl, CISSP, is the senior director for Campus Technology Services at the University of Notre Dame, where he has also taught cybersecurity and networking in the Mendoza College of Business. David has written multiple books on cybersecurity certification and cyberwarfare, and he has served as the technical editor for the sixth, seventh, and eighth editions of *CISSP Study Guide*. David holds a master's degree in information security and a bachelor's degree in communication technology from Eastern Michigan University, as well as CISSP, GPEN, GCIH, and CySA+ certifications.

Contents at a Glance

Introduction		*xxxiii*
Assessment Test		*xlii*
Chapter 1	Security Governance Through Principles and Policies	1
Chapter 2	Personnel Security and Risk Management Concepts	49
Chapter 3	Business Continuity Planning	97
Chapter 4	Laws, Regulations, and Compliance	125
Chapter 5	Protecting Security of Assets	159
Chapter 6	Cryptography and Symmetric Key Algorithms	195
Chapter 7	PKI and Cryptographic Applications	237
Chapter 8	Principles of Security Models, Design, and Capabilities	275
Chapter 9	Security Vulnerabilities, Threats, and Countermeasures	319
Chapter 10	Physical Security Requirements	399
Chapter 11	Secure Network Architecture and Securing Network Components	439
Chapter 12	Secure Communications and Network Attacks	521
Chapter 13	Managing Identity and Authentication	579
Chapter 14	Controlling and Monitoring Access	623
Chapter 15	Security Assessment and Testing	661
Chapter 16	Managing Security Operations	697
Chapter 17	Preventing and Responding to Incidents	737
Chapter 18	Disaster Recovery Planning	801
Chapter 19	Investigations and Ethics	845
Chapter 20	Software Development Security	871
Chapter 21	Malicious Code and Application Attacks	915
Appendix A	Answers to Review Questions	949
Appendix B	Answers to Written Labs	987
Index		*1001*

Contents

Introduction *xxxiii*

Assessment Test *xlii*

Chapter 1 Security Governance Through Principles and Policies 1

Understand and Apply Concepts of Confidentiality, Integrity, and Availability 2
- Confidentiality 3
- Integrity 4
- Availability 6
- Other Security Concepts 8
- Protection Mechanisms 12
- Layering 12
- Abstraction 13
- Data Hiding 13
- Encryption 14

Evaluate and Apply Security Governance Principles 14
- Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives 15
- Organizational Processes 17
- Organizational Roles and Responsibilities 23
- Security Control Frameworks 25
- Due Care and Due Diligence 26

Develop, Document, and Implement Security Policy, Standards, Procedures, and Guidelines 26
- Security Policies 26
- Security Standards, Baselines, and Guidelines 28
- Security Procedures 28

Understand and Apply Threat Modeling Concepts and Methodologies 30
- Identifying Threats 31
- Determining and Diagramming Potential Attacks 35
- Performing Reduction Analysis 36
- Prioritization and Response 37

Apply Risk-Based Management Concepts to the Supply Chain 38

Summary 40

Exam Essentials 42

Written Lab 44

Review Questions 45

Chapter 2 Personnel Security and Risk Management Concepts 49

Personnel Security Policies and Procedures 51
Candidate Screening and Hiring 55
Employment Agreements and Policies 55
Onboarding and Termination Processes 57
Vendor, Consultant, and Contractor Agreements and Controls 60
Compliance Policy Requirements 60
Privacy Policy Requirements 61
Security Governance 62
Understand and Apply Risk Management Concepts 63
Risk Terminology 64
Identify Threats and Vulnerabilities 67
Risk Assessment/Analysis 68
Risk Responses 76
Countermeasure Selection and Implementation 77
Applicable Types of Controls 79
Security Control Assessment 81
Monitoring and Measurement 81
Asset Valuation and Reporting 82
Continuous Improvement 83
Risk Frameworks 83
Establish and Maintain a Security Awareness, Education, and Training Program 86
Manage the Security Function 87
Summary 88
Exam Essentials 89
Written Lab 92
Review Questions 93

Chapter 3 Business Continuity Planning 97

Planning for Business Continuity 98
Project Scope and Planning 99
Business Organization Analysis 100
BCP Team Selection 101
Resource Requirements 103
Legal and Regulatory Requirements 104
Business Impact Assessment 105
Identify Priorities 106
Risk Identification 107
Likelihood Assessment 108
Impact Assessment 110
Resource Prioritization 111

Continuity Planning 111
Strategy Development 112
Provisions and Processes 112
Plan Approval and Implementation 114
Plan Approval 114
Plan Implementation 114
Training and Education 115
BCP Documentation 115
Summary 119
Exam Essentials 119
Written Lab 120
Review Questions 121

Chapter 4 Laws, Regulations, and Compliance 125

Categories of Laws 126
Criminal Law 126
Civil Law 128
Administrative Law 128
Laws 129
Computer Crime 129
Intellectual Property 134
Licensing 139
Import/Export 140
Privacy 141
Compliance 149
Contracting and Procurement 150
Summary 151
Exam Essentials 152
Written Lab 153
Review Questions 154

Chapter 5 Protecting Security of Assets 159

Identify and Classify Assets 160
Defining Sensitive Data 160
Defining Data Classifications 162
Defining Asset Classifications 165
Determining Data Security Controls 165
Understanding Data States 168
Handling Information and Assets 169
Data Protection Methods 176
Determining Ownership 178
Data Owners 179
Asset Owners 179

Business/Mission Owners 180
Data Processors 181
Administrators 184
Custodians 184
Users 185
Protecting Privacy 185
Using Security Baselines 186
Scoping and Tailoring 187
Selecting Standards 187
Summary 187
Exam Essentials 188
Written Lab 189
Review Questions 190

Chapter 6 Cryptography and Symmetric Key Algorithms 195

Historical Milestones in Cryptography 196
Caesar Cipher 196
American Civil War 197
Ultra vs. Enigma 198
Cryptographic Basics 198
Goals of Cryptography 198
Cryptography Concepts 200
Cryptographic Mathematics 202
Ciphers 207
Modern Cryptography 214
Cryptographic Keys 214
Symmetric Key Algorithms 215
Asymmetric Key Algorithms 216
Hashing Algorithms 219
Symmetric Cryptography 219
Data Encryption Standard 220
Triple DES 222
International Data Encryption Algorithm 223
Blowfish 223
Skipjack 223
Advanced Encryption Standard 224
Symmetric Key Management 226
Cryptographic Lifecycle 228
Summary 229
Exam Essentials 229
Written Lab 231
Review Questions 232

Chapter 7 PKI and Cryptographic Applications 237

Asymmetric Cryptography 238
Public and Private Keys 238
RSA 239
El Gamal 241
Elliptic Curve 242
Hash Functions 242
SHA 244
MD2 244
MD4 245
MD5 245
Digital Signatures 246
HMAC 247
Digital Signature Standard 248
Public Key Infrastructure 249
Certificates 249
Certificate Authorities 250
Certificate Generation and Destruction 251
Asymmetric Key Management 253
Applied Cryptography 254
Portable Devices 254
Email 255
Web Applications 256
Digital Rights Management 259
Networking 262
Cryptographic Attacks 265
Summary 268
Exam Essentials 269
Written Lab 270
Review Questions 271

Chapter 8 Principles of Security Models, Design, and Capabilities 275

Implement and Manage Engineering Processes Using Secure Design Principles 276
Objects and Subjects 277
Closed and Open Systems 277
Techniques for Ensuring Confidentiality, Integrity, and Availability 279
Controls 280
Trust and Assurance 281
Understand the Fundamental Concepts of Security Models 281
Trusted Computing Base 282
State Machine Model 284

Information Flow Model 285
Noninterference Model 285
Take-Grant Model 286
Access Control Matrix 286
Bell-LaPadula Model 288
Biba Model 290
Clark-Wilson Model 292
Brewer and Nash Model (aka Chinese Wall) 293
Goguen-Meseguer Model 294
Sutherland Model 294
Graham-Denning Model 294
Select Controls Based On Systems Security Requirements 295
Rainbow Series 296
ITSEC Classes and Required Assurance and Functionality 301
Common Criteria 302
Industry and International Security Implementation Guidelines 305
Certification and Accreditation 306
Understand Security Capabilities of Information Systems 309
Memory Protection 309
Virtualization 310
Trusted Platform Module 310
Interfaces 311
Fault Tolerance 311
Summary 311
Exam Essentials 312
Written Lab 313
Review Questions 314

Chapter 9 Security Vulnerabilities, Threats, and Countermeasures 319

Assess and Mitigate Security Vulnerabilities 320
Hardware 321
Firmware 341
Client-Based Systems 342
Applets 342
Local Caches 344
Server-Based Systems 346
Database Systems Security 347
Aggregation 347
Inference 348
Data Mining and Data Warehousing 348
Data Analytics 349
Large-Scale Parallel Data Systems 350

Distributed Systems and Endpoint Security 350
Cloud-Based Systems and Cloud Computing 353
Grid Computing 357
Peer to Peer 358
Internet of Things 358
Industrial Control Systems 359
Assess and Mitigate Vulnerabilities in Web-Based Systems 360
Assess and Mitigate Vulnerabilities in Mobile Systems 365
Device Security 366
Application Security 370
BYOD Concerns 372
Assess and Mitigate Vulnerabilities in Embedded Devices and Cyber-Physical Systems 375
Examples of Embedded and Static Systems 376
Methods of Securing Embedded and Static Systems 377
Essential Security Protection Mechanisms 379
Technical Mechanisms 380
Security Policy and Computer Architecture 383
Policy Mechanisms 383
Common Architecture Flaws and Security Issues 384
Covert Channels 385
Attacks Based on Design or Coding Flaws and Security Issues 385
Programming 388
Timing, State Changes, and Communication Disconnects 389
Technology and Process Integration 389
Electromagnetic Radiation 389
Summary 390
Exam Essentials 391
Written Lab 394
Review Questions 395

Chapter 10 Physical Security Requirements 399

Apply Security Principles to Site and Facility Design 400
Secure Facility Plan 401
Site Selection 401
Visibility 402
Natural Disasters 402
Facility Design 402
Implement Site and Facility Security Controls 403
Equipment Failure 404
Wiring Closets 405
Server Rooms/Data Centers 407
Media Storage Facilities 412

Evidence Storage 413
Restricted and Work Area Security 413
Utilities and HVAC Considerations 414
Fire Prevention, Detection, and Suppression 417
Implement and Manage Physical Security 422
Perimeter Security Controls 422
Internal Security Controls 425
Summary 431
Exam Essentials 432
Written Lab 434
Review Questions 435

Chapter 11 Secure Network Architecture and Securing Network Components 439

OSI Model 440
History of the OSI Model 441
OSI Functionality 441
Encapsulation/Deencapsulation 442
OSI Layers 444
TCP/IP Model 451
TCP/IP Protocol Suite Overview 452
Converged Protocols 470
Content Distribution Networks 472
Wireless Networks 472
Securing Wireless Access Points 473
Securing the SSID 475
Conducting a Site Survey 476
Using Secure Encryption Protocols 476
Determining Antenna Placement 479
Antenna Types 480
Adjusting Power Level Controls 480
WPS 481
Using Captive Portals 481
General Wi-Fi Security Procedure 481
Wireless Attacks 482
Secure Network Components 486
Network Access Control 487
Firewalls 487
Endpoint Security 491
Secure Operation of Hardware 492
Cabling, Wireless, Topology, Communications, and Transmission Media Technology 495
Transmission Media 496
Network Topologies 500

Wireless Communications and Security 503
LAN Technologies 509
Summary 513
Exam Essentials 514
Written Lab 516
Review Questions 517

Chapter 12 Secure Communications and Network Attacks 521

Network and Protocol Security Mechanisms 522
Secure Communications Protocols 523
Authentication Protocols 524
Secure Voice Communications 525
Voice over Internet Protocol (VoIP) 525
Social Engineering 526
Fraud and Abuse 527
Multimedia Collaboration 529
Remote Meeting 529
Instant Messaging 530
Manage Email Security 530
Email Security Goals 531
Understand Email Security Issues 532
Email Security Solutions 533
Remote Access Security Management 536
Plan Remote Access Security 538
Dial-Up Protocols 539
Centralized Remote Authentication Services 540
Virtual Private Network 540
Tunneling 541
How VPNs Work 542
Common VPN Protocols 543
Virtual LAN 545
Virtualization 546
Virtual Software 547
Virtual Networking 548
Network Address Translation 549
Private IP Addresses 550
Stateful NAT 551
Static and Dynamic NAT 552
Automatic Private IP Addressing 552
Switching Technologies 553
Circuit Switching 554
Packet Switching 554
Virtual Circuits 555

WAN Technologies 556
WAN Connection Technologies 558
Dial-Up Encapsulation Protocols 561
Miscellaneous Security Control Characteristics 561
Transparency 561
Verify Integrity 562
Transmission Mechanisms 563
Security Boundaries 563
Prevent or Mitigate Network Attacks 564
DoS and DDoS 564
Eavesdropping 565
Impersonation/Masquerading 566
Replay Attacks 567
Modification Attacks 567
Address Resolution Protocol Spoofing 567
DNS Poisoning, Spoofing, and Hijacking 568
Hyperlink Spoofing 568
Summary 569
Exam Essentials 571
Written Lab 573
Review Questions 574

Chapter 13 Managing Identity and Authentication 579

Controlling Access to Assets 580
Comparing Subjects and Objects 581
The CIA Triad and Access Controls 581
Types of Access Control 582
Comparing Identification and Authentication 584
Registration and Proofing of Identity 585
Authorization and Accountability 586
Authentication Factors 587
Passwords 588
Smartcards and Tokens 592
Biometrics 595
Multifactor Authentication 599
Device Authentication 600
Service Authentication 601
Implementing Identity Management 602
Single Sign-On 602
Credential Management Systems 607
Integrating Identity Services 608
Managing Sessions 608
AAA Protocols 609

Managing the Identity and Access Provisioning Lifecycle 611
Provisioning 611
Account Review 612
Account Revocation 613
Summary 614
Exam Essentials 615
Written Lab 617
Review Questions 618

Chapter 14 Controlling and Monitoring Access 623

Comparing Access Control Models 624
Comparing Permissions, Rights, and Privileges 624
Understanding Authorization Mechanisms 625
Defining Requirements with a Security Policy 626
Implementing Defense in Depth 627
Summarizing Access Control Models 628
Discretionary Access Controls 629
Nondiscretionary Access Controls 630
Understanding Access Control Attacks 635
Risk Elements 636
Identifying Assets 637
Identifying Threats 638
Identifying Vulnerabilities 640
Common Access Control Attacks 641
Summary of Protection Methods 652
Summary 653
Exam Essentials 654
Written Lab 656
Review Questions 657

Chapter 15 Security Assessment and Testing 661

Building a Security Assessment and Testing Program 662
Security Testing 662
Security Assessments 664
Security Audits 665
Performing Vulnerability Assessments 668
Describing Vulnerabilities 668
Vulnerability Scans 668
Penetration Testing 679
Testing Your Software 681
Code Review and Testing 682
Interface Testing 686
Misuse Case Testing 686

Test Coverage Analysis 686
Website Monitoring 687
Implementing Security Management Processes 688
Log Reviews 688
Account Management 689
Backup Verification 689
Key Performance and Risk Indicators 690
Summary 690
Exam Essentials 691
Written Lab 692
Review Questions 693

Chapter 16 Managing Security Operations 697

Applying Security Operations Concepts 698
Need-to-Know and Least Privilege 698
Separation of Duties and Responsibilities 700
Job Rotation 703
Mandatory Vacations 703
Privileged Account Management 704
Managing the Information Lifecycle 706
Service-Level Agreements 707
Addressing Personnel Safety and Security 708
Securely Provisioning Resources 710
Managing Hardware and Software Assets 710
Protecting Physical Assets 711
Managing Virtual Assets 712
Managing Cloud-Based Assets 713
Media Management 714
Managing Configuration 718
Baselining 718
Using Images for Baselining 718
Managing Change 719
Security Impact Analysis 721
Versioning 722
Configuration Documentation 723
Managing Patches and Reducing Vulnerabilities 723
Systems to Manage 723
Patch Management 724
Vulnerability Management 725
Common Vulnerabilities and Exposures 728
Summary 728
Exam Essentials 729
Written Lab 731
Review Questions 732

Chapter 17 Preventing and Responding to Incidents 737

Managing Incident Response 738
Defining an Incident 738
Incident Response Steps 739
Implementing Detective and Preventive Measures 745
Basic Preventive Measures 745
Understanding Attacks 746
Intrusion Detection and Prevention Systems 756
Specific Preventive Measures 763
Logging, Monitoring, and Auditing 773
Logging and Monitoring 773
Egress Monitoring 781
Auditing to Assess Effectiveness 783
Security Audits and Reviews 787
Reporting Audit Results 788
Summary 790
Exam Essentials 792
Written Lab 795
Review Questions 796

Chapter 18 Disaster Recovery Planning 801

The Nature of Disaster 802
Natural Disasters 803
Man-Made Disasters 807
Understand System Resilience and Fault Tolerance 812
Protecting Hard Drives 813
Protecting Servers 814
Protecting Power Sources 815
Trusted Recovery 816
Quality of Service 817
Recovery Strategy 818
Business Unit and Functional Priorities 818
Crisis Management 819
Emergency Communications 820
Workgroup Recovery 820
Alternate Processing Sites 820
Mutual Assistance Agreements 825
Database Recovery 825
Recovery Plan Development 827
Emergency Response 828
Personnel and Communications 828
Assessment 829
Backups and Offsite Storage 829

Software Escrow Arrangements 833
External Communications 833
Utilities 834
Logistics and Supplies 834
Recovery vs. Restoration 834
Training, Awareness, and Documentation 835
Testing and Maintenance 836
Read-Through Test 836
Structured Walk-Through 837
Simulation Test 837
Parallel Test 837
Full-Interruption Test 837
Maintenance 837
Summary 838
Exam Essentials 838
Written Lab 839
Review Questions 840

Chapter 19 Investigations and Ethics 845

Investigations 846
Investigation Types 846
Evidence 849
Investigation Process 853
Major Categories of Computer Crime 857
Military and Intelligence Attacks 857
Business Attacks 858
Financial Attacks 859
Terrorist Attacks 859
Grudge Attacks 859
Thrill Attacks 861
Ethics 861
$(ISC)^2$ Code of Ethics 862
Ethics and the Internet 862
Summary 864
Exam Essentials 864
Written Lab 865
Review Questions 866

Chapter 20 Software Development Security 871

Introducing Systems Development Controls 872
Software Development 872
Systems Development Lifecycle 878
Lifecycle Models 881