

# (ISC)<sup>2</sup>®



## Certified Information Systems Security Professional

### Official Study Guide

#### Ninth Edition

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

**Covers all of the 2021 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 1,000 practice questions and exercises
- More than 700 electronic flashcards
- Searchable key term glossary
- 2 hour and 50 minute audio review of Exam Essentials





**(ISC)<sup>2</sup>®**

**CISSP® Certified Information  
Systems Security Professional  
Official Study Guide**

**Ninth Edition**





**(ISC)<sup>2</sup>®**

**CISSP® Certified Information  
Systems Security Professional  
Official Study Guide**

**Ninth Edition**



Mike Chapple

James Michael Stewart

Darril Gibson

 **SYBEX**  
A Wiley Brand

Copyright © 2021 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey

Published simultaneously in Canada and the United Kingdom

ISBN: 978-1-119-78623-8

ISBN: 978-1-119-78633-7 (ebk)

ISBN: 978-1-119-78624-5 (ebk)

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at <http://www.wiley.com/go/permissions>.

**Limit of Liability/Disclaimer of Warranty:** While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at [www.wiley.com](http://www.wiley.com).

**Library of Congress Control Number:** 2021935479

**TRADEMARKS:** WILEY and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. (ISC)<sup>2</sup> and CISSP are trademarks or registered trademarks of (ISC)<sup>2</sup>, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

Cover image(s): © Jeremy Woodhouse/Getty Images, Inc.

Cover design: Wiley

*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 29 years and letting me share mine with you.*  
—Darril Gibson





# Acknowledgments

We'd like to express our thanks to Wiley for continuing to support this project. Extra thanks to the development editor, Kelly Talbot, and technical editors, Jerry Rayome, Chris Crayton, and Aaron Kraus, 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 my many friends and colleagues in the cybersecurity community 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 and I'd like to thank them both for their thoughtful contributions to my chapters.

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

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, Jerry Rayome, Chris Crayton, and Aaron Kraus, provided us with some outstanding feedback, and this book is better because of their efforts. Thanks to the team at Wiley (including project managers, editors, and graphic 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, PhD,** CISSP, Security+, CySA+, PenTest+, CISA, CISM, CCSP, CIPP/US, is a 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)<sup>2</sup> Practice Tests*, *CompTIA CySA+ Study Guide: Exam CS0-001*, *CompTIA Security+ Study Guide: Exam SY0-601*, 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](http://www.certmike.com).

**James Michael Stewart,** CISSP, CEH, CHFI, ECSA, CND, ECIH, CySA+, PenTest+, CASP+, Security+, Network+, A+, CISM, and CFR, has been writing and training for more than 25 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 on security certification, Microsoft topics, and network administration, including *CompTIA Security+ Review Guide: Exam SY0-601*. More information about Michael can be found at his website at [www.impactonline.com](http://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 [blogs.getcertifiedgetahead.com](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

**Jerry Rayome**, BS/MS Computer Science, CISSP, has been employed as a member of the Cyber Security Program at Lawrence Livermore National Laboratory for over 20 years, providing cybersecurity services that include software development, penetrative testing, incident response, firewall implementation/administration, firewall auditing, honeynet deployment/monitoring, cyber forensic investigations, NIST 800-53 control implementation/assessment, cloud risk assessment, and cloud security auditing.

**Chris Crayton** is a technical consultant, trainer, author, and industry-leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several leading publishing companies. He holds numerous industry certifications, including CISSP, MCSE, CompTIA S+, N+, A+, and many others. He has also been recognized with many professional and teaching awards, and he has served as a state-level SkillsUSA final competition judge.

**Aaron Kraus**, CISSP, CCSP, is an information security practitioner, instructor, and author who has worked across industries and around the world. He has spent more than 15 years as a consultant or security risk manager in roles with government, financial services, and tech startups, including most recently in cyber risk insurance, and has spent 13 years teaching, writing, and developing security courseware at Learning Tree International, where he is also dean of cybersecurity curriculum. His writing and editing experience includes official (ISC)<sup>2</sup> reference books, practice exams, and study guides for both CISSP and CCSP.



# Contents at a Glance

<i>Introduction</i>		<i>xxxvii</i>
<i>Assessment Test</i>		<i>lix</i>
<b>Chapter 1</b>	Security Governance Through Principles and Policies	1
<b>Chapter 2</b>	Personnel Security and Risk Management Concepts	43
<b>Chapter 3</b>	Business Continuity Planning	113
<b>Chapter 4</b>	Laws, Regulations, and Compliance	143
<b>Chapter 5</b>	Protecting Security of Assets	179
<b>Chapter 6</b>	Cryptography and Symmetric Key Algorithms	219
<b>Chapter 7</b>	PKI and Cryptographic Applications	263
<b>Chapter 8</b>	Principles of Security Models, Design, and Capabilities	309
<b>Chapter 9</b>	Security Vulnerabilities, Threats, and Countermeasures	353
<b>Chapter 10</b>	Physical Security Requirements	447
<b>Chapter 11</b>	Secure Network Architecture and Components	495
<b>Chapter 12</b>	Secure Communications and Network Attacks	581
<b>Chapter 13</b>	Managing Identity and Authentication	637
<b>Chapter 14</b>	Controlling and Monitoring Access	677
<b>Chapter 15</b>	Security Assessment and Testing	723
<b>Chapter 16</b>	Managing Security Operations	763
<b>Chapter 17</b>	Preventing and Responding to Incidents	801
<b>Chapter 18</b>	Disaster Recovery Planning	861
<b>Chapter 19</b>	Investigations and Ethics	909
<b>Chapter 20</b>	Software Development Security	941
<b>Chapter 21</b>	Malicious Code and Application Attacks	993
<b>Appendix A</b>	Answers to Review Questions	1041
<b>Appendix B</b>	Answers to Written Labs	1099
<i>Index</i>		<i>1117</i>





# Contents

<i>Introduction</i>	<i>xxxvii</i>
<i>Assessment Test</i>	<i>lix</i>
<b>Chapter 1</b>	<b>Security Governance Through Principles and Policies 1</b>
Security 101	3
Understand and Apply Security Concepts	4
Confidentiality	5
Integrity	6
Availability	7
DAD, Overprotection, Authenticity, Non-repudiation, and AAA Services	7
Protection Mechanisms	11
Security Boundaries	13
Evaluate and Apply Security Governance Principles	14
Third-Party Governance	15
Documentation Review	15
Manage the Security Function	16
Alignment of Security Function to Business Strategy, Goals, Mission, and Objectives	17
Organizational Processes	19
Organizational Roles and Responsibilities	21
Security Control Frameworks	22
Due Diligence and Due Care	23
Security Policy, Standards, Procedures, and Guidelines	23
Security Policies	24
Security Standards, Baselines, and Guidelines	24
Security Procedures	25
Threat Modeling	26
Identifying Threats	26
Determining and Diagramming Potential Attacks	28
Performing Reduction Analysis	28
Prioritization and Response	30
Supply Chain Risk Management	31
Summary	33
Exam Essentials	33
Written Lab	36
Review Questions	37

<b>Chapter 2</b>	<b>Personnel Security and Risk Management Concepts</b>	<b>43</b>
	Personnel Security Policies and Procedures	45
	Job Descriptions and Responsibilities	45
	Candidate Screening and Hiring	46
	Onboarding: Employment Agreements and Policies	47
	Employee Oversight	48
	Offboarding, Transfers, and Termination Processes	49
	Vendor, Consultant, and Contractor Agreements and Controls	52
	Compliance Policy Requirements	53
	Privacy Policy Requirements	54
	Understand and Apply Risk Management Concepts	55
	Risk Terminology and Concepts	56
	Asset Valuation	58
	Identify Threats and Vulnerabilities	60
	Risk Assessment/Analysis	60
	Risk Responses	66
	Cost vs. Benefit of Security Controls	69
	Countermeasure Selection and Implementation	72
	Applicable Types of Controls	74
	Security Control Assessment	76
	Monitoring and Measurement	76
	Risk Reporting and Documentation	77
	Continuous Improvement	77
	Risk Frameworks	79
	Social Engineering	81
	Social Engineering Principles	83
	Eliciting Information	85
	Prepending	85
	Phishing	85
	Spear Phishing	87
	Whaling	87
	Smishing	88
	Vishing	88
	Spam	89
	Shoulder Surfing	90
	Invoice Scams	90
	Hoax	90
	Impersonation and Masquerading	91
	Tailgating and Piggybacking	91
	Dumpster Diving	92
	Identity Fraud	93
	Typo Squatting	94
	Influence Campaigns	94

Establish and Maintain a Security Awareness, Education, and Training Program	96
Awareness	97
Training	97
Education	98
Improvements	98
Effectiveness Evaluation	99
Summary	100
Exam Essentials	101
Written Lab	106
Review Questions	107

**Chapter 3 Business Continuity Planning 113**

Planning for Business Continuity	114
Project Scope and Planning	115
Organizational Review	116
BCP Team Selection	117
Resource Requirements	119
Legal and Regulatory Requirements	120
Business Impact Analysis	121
Identifying Priorities	122
Risk Identification	123
Likelihood Assessment	125
Impact Analysis	126
Resource Prioritization	128
Continuity Planning	128
Strategy Development	129
Provisions and Processes	129
Plan Approval and Implementation	131
Plan Approval	131
Plan Implementation	132
Training and Education	132
BCP Documentation	132
Summary	136
Exam Essentials	137
Written Lab	138
Review Questions	139

**Chapter 4 Laws, Regulations, and Compliance 143**

Categories of Laws	144
Criminal Law	144
Civil Law	146
Administrative Law	146
Laws	147
Computer Crime	147
Intellectual Property (IP)	152

	Licensing	158
	Import/Export	158
	Privacy	160
	State Privacy Laws	168
	Compliance	169
	Contracting and Procurement	171
	Summary	171
	Exam Essentials	172
	Written Lab	173
	Review Questions	174
<b>Chapter 5</b>	<b>Protecting Security of Assets</b>	<b>179</b>
	Identifying and Classifying Information and Assets	180
	Defining Sensitive Data	180
	Defining Data Classifications	182
	Defining Asset Classifications	185
	Understanding Data States	185
	Determining Compliance Requirements	186
	Determining Data Security Controls	186
	Establishing Information and Asset Handling Requirements	188
	Data Maintenance	189
	Data Loss Prevention	189
	Marking Sensitive Data and Assets	190
	Handling Sensitive Information and Assets	192
	Data Collection Limitation	192
	Data Location	193
	Storing Sensitive Data	193
	Data Destruction	194
	Ensuring Appropriate Data and Asset Retention	197
	Data Protection Methods	199
	Digital Rights Management	199
	Cloud Access Security Broker	200
	Pseudonymization	200
	Tokenization	201
	Anonymization	202
	Understanding Data Roles	204
	Data Owners	204
	Asset Owners	205
	Business/Mission Owners	206
	Data Processors and Data Controllers	206
	Data Custodians	207
	Administrators	207
	Users and Subjects	208

	Using Security Baselines	208
	Comparing Tailoring and Scoping	209
	Standards Selection	210
	Summary	211
	Exam Essentials	211
	Written Lab	213
	Review Questions	214
<b>Chapter 6</b>	<b>Cryptography and Symmetric Key Algorithms</b>	<b>219</b>
	Cryptographic Foundations	220
	Goals of Cryptography	220
	Cryptography Concepts	223
	Cryptographic Mathematics	224
	Ciphers	230
	Modern Cryptography	238
	Cryptographic Keys	238
	Symmetric Key Algorithms	239
	Asymmetric Key Algorithms	241
	Hashing Algorithms	244
	Symmetric Cryptography	244
	Cryptographic Modes of Operation	245
	Data Encryption Standard	247
	Triple DES	247
	International Data Encryption Algorithm	248
	Blowfish	249
	Skipjack	249
	Rivest Ciphers	249
	Advanced Encryption Standard	250
	CAST	250
	Comparison of Symmetric Encryption Algorithms	251
	Symmetric Key Management	252
	Cryptographic Lifecycle	255
	Summary	255
	Exam Essentials	256
	Written Lab	257
	Review Questions	258
<b>Chapter 7</b>	<b>PKI and Cryptographic Applications</b>	<b>263</b>
	Asymmetric Cryptography	264
	Public and Private Keys	264
	RSA	265
	ElGamal	267
	Elliptic Curve	268
	Diffie–Hellman Key Exchange	269
	Quantum Cryptography	270

Hash Functions	271
SHA	272
MD5	273
RIPEMD	273
Comparison of Hash Algorithm Value Lengths	274
Digital Signatures	275
HMAC	276
Digital Signature Standard	277
Public Key Infrastructure	277
Certificates	278
Certificate Authorities	279
Certificate Lifecycle	280
Certificate Formats	283
Asymmetric Key Management	284
Hybrid Cryptography	285
Applied Cryptography	285
Portable Devices	285
Email	286
Web Applications	290
Steganography and Watermarking	292
Networking	294
Emerging Applications	295
Cryptographic Attacks	297
Summary	301
Exam Essentials	302
Written Lab	303
Review Questions	304
<b>Chapter 8</b>	
<b>Principles of Security Models, Design, and Capabilities</b>	<b>309</b>
Secure Design Principles	310
Objects and Subjects	311
Closed and Open Systems	312
Secure Defaults	314
Fail Securely	314
Keep It Simple	316
Zero Trust	317
Privacy by Design	319
Trust but Verify	319
Techniques for Ensuring CIA	320
Confinement	320
Bounds	320
Isolation	321
Access Controls	321
Trust and Assurance	321

Understand the Fundamental Concepts of Security Models	322
Trusted Computing Base	323
State Machine Model	325
Information Flow Model	325
Noninterference Model	326
Take-Grant Model	326
Access Control Matrix	327
Bell–LaPadula Model	328
Biba Model	330
Clark–Wilson Model	333
Brewer and Nash Model	334
Goguen–Meseguer Model	335
Sutherland Model	335
Graham–Denning Model	335
Harrison–Ruzzo–Ullman Model	336
Select Controls Based on Systems Security Requirements	337
Common Criteria	337
Authorization to Operate	340
Understand Security Capabilities of Information Systems	341
Memory Protection	341
Virtualization	342
Trusted Platform Module	342
Interfaces	343
Fault Tolerance	343
Encryption/Decryption	343
Summary	343
Exam Essentials	344
Written Lab	347
Review Questions	348

**Chapter 9      Security Vulnerabilities, Threats, and Countermeasures      353**

Shared Responsibility	354
Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements	355
Hardware	356
Firmware	370
Client-Based Systems	372
Mobile Code	372
Local Caches	375
Server-Based Systems	375
Large-Scale Parallel Data Systems	376
Grid Computing	377
Peer to Peer	378

Industrial Control Systems	378
Distributed Systems	380
High-Performance Computing (HPC) Systems	382
Internet of Things	383
Edge and Fog Computing	385
Embedded Devices and Cyber-Physical Systems	386
Static Systems	387
Network-Enabled Devices	388
Cyber-Physical Systems	389
Elements Related to Embedded and Static Systems	389
Security Concerns of Embedded and Static Systems	390
Specialized Devices	393
Microservices	394
Infrastructure as Code	395
Virtualized Systems	397
Virtual Software	399
Virtualized Networking	400
Software-Defined Everything	400
Virtualization Security Management	403
Containerization	405
Serverless Architecture	406
Mobile Devices	406
Mobile Device Security Features	408
Mobile Device Deployment Policies	420
Essential Security Protection Mechanisms	426
Process Isolation	426
Hardware Segmentation	427
System Security Policy	427
Common Security Architecture Flaws and Issues	428
Covert Channels	428
Attacks Based on Design or Coding Flaws	430
Rootkits	431
Incremental Attacks	431
Summary	432
Exam Essentials	433
Written Lab	440
Review Questions	441
<b>Chapter 10 Physical Security Requirements</b>	<b>447</b>
Apply Security Principles to Site and Facility Design	448
Secure Facility Plan	448
Site Selection	449
Facility Design	450



Implement Site and Facility Security Controls	452
Equipment Failure	453
Wiring Closets	454
Server Rooms/Data Centers	455
Intrusion Detection Systems	458
Cameras	460
Access Abuses	462
Media Storage Facilities	462
Evidence Storage	463
Restricted and Work Area Security	464
Utility Considerations	465
Fire Prevention, Detection, and Suppression	470
Implement and Manage Physical Security	476
Perimeter Security Controls	477
Internal Security Controls	481
Key Performance Indicators of Physical Security	483
Summary	484
Exam Essentials	485
Written Lab	488
Review Questions	489
<b>Chapter 11</b>	<b>Secure Network Architecture and Components</b>
	<b>495</b>
OSI Model	497
History of the OSI Model	497
OSI Functionality	498
Encapsulation/Deencapsulation	498
OSI Layers	500
TCP/IP Model	504
Analyzing Network Traffic	505
Common Application Layer Protocols	506
Transport Layer Protocols	508
Domain Name System	509
DNS Poisoning	511
Domain Hijacking	514
Internet Protocol (IP) Networking	516
IPv4 vs. IPv6	516
IP Classes	517
ICMP	519
IGMP	519
ARP Concerns	519
Secure Communication Protocols	521
Implications of Multilayer Protocols	522
Converged Protocols	523
Voice over Internet Protocol (VoIP)	524
Software-Defined Networking	525

Microsegmentation	526
Wireless Networks	527
Securing the SSID	529
Wireless Channels	529
Conducting a Site Survey	530
Wireless Security	531
Wi-Fi Protected Setup (WPS)	533
Wireless MAC Filter	534
Wireless Antenna Management	534
Using Captive Portals	535
General Wi-Fi Security Procedure	535
Wireless Communications	536
Wireless Attacks	539
Other Communication Protocols	543
Cellular Networks	544
Content Distribution Networks (CDNs)	545
Secure Network Components	545
Secure Operation of Hardware	546
Common Network Equipment	547
Network Access Control	549
Firewalls	550
Endpoint Security	556
Cabling, Topology, and Transmission Media Technology	559
Transmission Media	559
Network Topologies	563
Ethernet	565
Sub-Technologies	566
Summary	569
Exam Essentials	570
Written Lab	574
Review Questions	575
<b>Chapter 12</b>	<b>Secure Communications and Network Attacks</b>
	<b>581</b>
Protocol Security Mechanisms	582
Authentication Protocols	582
Port Security	585
Quality of Service (QoS)	585
Secure Voice Communications	586
Public Switched Telephone Network	586
Voice over Internet Protocol (VoIP)	586
Vishing and Phreaking	588
PBX Fraud and Abuse	589
Remote Access Security Management	590
Remote Access and Telecommuting Techniques	591
Remote Connection Security	591
Plan a Remote Access Security Policy	592

Multimedia Collaboration	593
Remote Meeting	593
Instant Messaging and Chat	594
Load Balancing	595
Virtual IPs and Load Persistence	596
Active-Active vs. Active-Passive	596
Manage Email Security	596
Email Security Goals	597
Understand Email Security Issues	599
Email Security Solutions	599
Virtual Private Network	602
Tunneling	603
How VPNs Work	604
Always-On	606
Split Tunnel vs. Full Tunnel	607
Common VPN Protocols	607
Switching and Virtual LANs	610
Network Address Translation	614
Private IP Addresses	616
Stateful NAT	617
Automatic Private IP Addressing	617
Third-Party Connectivity	618
Switching Technologies	620
Circuit Switching	620
Packet Switching	620
Virtual Circuits	621
WAN Technologies	622
Fiber-Optic Links	624
Security Control Characteristics	624
Transparency	625
Transmission Management Mechanisms	625
Prevent or Mitigate Network Attacks	625
Eavesdropping	626
Modification Attacks	626
Summary	626
Exam Essentials	628
Written Lab	630
Review Questions	631
<b>Chapter 13</b>	<b>Managing Identity and Authentication</b>
	<b>637</b>
Controlling Access to Assets	639
Controlling Physical and Logical Access	640
The CIA Triad and Access Controls	640
Managing Identification and Authentication	641
Comparing Subjects and Objects	642

Registration, Proofing, and Establishment of Identity	643
Authorization and Accountability	644
Authentication Factors Overview	645
Something You Know	647
Something You Have	650
Something You Are	651
Multifactor Authentication (MFA)	655
Two-Factor Authentication with Authenticator Apps	655
Passwordless Authentication	656
Device Authentication	657
Service Authentication	658
Mutual Authentication	659
Implementing Identity Management	659
Single Sign-On	659
SSO and Federated Identities	660
Credential Management Systems	662
Credential Manager Apps	663
Scripted Access	663
Session Management	663
Managing the Identity and Access Provisioning Lifecycle	664
Provisioning and Onboarding	665
Deprovisioning and Offboarding	666
Defining New Roles	667
Account Maintenance	667
Account Access Review	667
Summary	668
Exam Essentials	669
Written Lab	671
Review Questions	672
<b>Chapter 14</b>	<b>Controlling and Monitoring Access</b>
	<b>677</b>
Comparing Access Control Models	678
Comparing Permissions, Rights, and Privileges	678
Understanding Authorization Mechanisms	679
Defining Requirements with a Security Policy	681
Introducing Access Control Models	681
Discretionary Access Control	682
Nondiscretionary Access Control	683
Implementing Authentication Systems	690
Implementing SSO on the Internet	691
Implementing SSO on Internal Networks	694
Understanding Access Control Attacks	699
Risk Elements	700
Common Access Control Attacks	700
Core Protection Methods	713

	Summary	714
	Exam Essentials	715
	Written Lab	717
	Review Questions	718
<b>Chapter 15</b>	<b>Security Assessment and Testing</b>	<b>723</b>
	Building a Security Assessment and Testing Program	725
	Security Testing	725
	Security Assessments	726
	Security Audits	727
	Performing Vulnerability Assessments	731
	Describing Vulnerabilities	731
	Vulnerability Scans	732
	Penetration Testing	742
	Compliance Checks	745
	Testing Your Software	746
	Code Review and Testing	746
	Interface Testing	751
	Misuse Case Testing	751
	Test Coverage Analysis	752
	Website Monitoring	752
	Implementing Security Management Processes	753
	Log Reviews	753
	Account Management	754
	Disaster Recovery and Business Continuity	754
	Training and Awareness	755
	Key Performance and Risk Indicators	755
	Summary	756
	Exam Essentials	756
	Written Lab	758
	Review Questions	759
<b>Chapter 16</b>	<b>Managing Security Operations</b>	<b>763</b>
	Apply Foundational Security Operations Concepts	765
	Need to Know and Least Privilege	765
	Separation of Duties (SoD) and Responsibilities	767
	Two-Person Control	768
	Job Rotation	768
	Mandatory Vacations	768
	Privileged Account Management	769
	Service Level Agreements (SLAs)	771
	Addressing Personnel Safety and Security	771
	Duress	771
	Travel	772

Emergency Management	773
Security Training and Awareness	773
Provision Resources Securely	773
Information and Asset Ownership	774
Asset Management	774
Apply Resource Protection	776
Media Management	776
Media Protection Techniques	776
Managed Services in the Cloud	779
Shared Responsibility with Cloud Service Models	780
Scalability and Elasticity	782
Perform Configuration Management (CM)	782
Provisioning	783
Baselining	783
Using Images for Baselining	783
Automation	784
Managing Change	785
Change Management	787
Versioning	788
Configuration Documentation	788
Managing Patches and Reducing Vulnerabilities	789
Systems to Manage	789
Patch Management	789
Vulnerability Management	791
Vulnerability Scans	792
Common Vulnerabilities and Exposures	792
Summary	793
Exam Essentials	794
Written Lab	796
Review Questions	797
<b>Chapter 17</b>	<b>Preventing and Responding to Incidents</b>
	<b>801</b>
Conducting Incident Management	803
Defining an Incident	803
Incident Management Steps	804
Implementing Detective and Preventive Measures	810
Basic Preventive Measures	810
Understanding Attacks	811
Intrusion Detection and Prevention Systems	820
Specific Preventive Measures	828
Logging and Monitoring	834
Logging Techniques	834
The Role of Monitoring	837
Monitoring Techniques	840