

ISC2 

Certified Information
Systems Security Professional

OFFICIAL STUDY GUIDE

Tenth Edition

COVERS ALL OF THE 2024 UPDATED CISSP OBJECTIVES

Includes interactive online learning environment and study tools with:

- **More than 900 practice questions and exercises**
- **More than 1,000 electronic flashcards**
- **Searchable key term glossary**
- **More than 2 hours of Study Essentials Audio Review**

Mike Chapple, CISSP

James Michael Stewart, CISSP

Darril Gibson, CISSP

 **SYBEX**
A Wiley Brand

ISC2[®] CISSP[®]

**Certified Information
Systems Security
Professional**

Official Study Guide

Tenth Edition



ISC2® CISSP®

Certified Information Systems Security Professional

Official Study Guide
Tenth Edition



Mike Chapple, CISSP

James Michael Stewart, CISSP

Darril Gibson, CISSP



Copyright © 2024 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.

ISBNs: 9781394254699 (paperback), 9781394254712 (ePDF), 9781394254705 (ePub)

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 Section 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, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. 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 www.wiley.com/go/permission.

Trademarks: WILEY, the Wiley logo, and the Sybex 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. ISC2 and CISSP are trademarks or registered trademarks of International Information Systems Security Certification Consortium, 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.

Limit of Liability/Disclaimer of Warranty: While the publisher and authors 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. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors 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, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993. For product technical support, you can find answers to frequently asked questions or reach us via live chat at <https://sybexsupport.wiley.com>.

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.

Library of Congress Control Number: 2024935047

Cover image: © Getty Images Inc./Jeremy Woodhouse

Cover design: Wiley

To Darril Gibson, my friend and co-author of many years. You made a tremendous impact on the cybersecurity field and we will be eternally grateful for your contributions.

—Mike Chapple

To Cathy, I continue to love threading the zigzaggednesses of life with you.

—James Michael Stewart

Acknowledgments

We'd like to express our thanks to Sybex for continuing to support this project. Extra thanks to the tenth edition developmental editor, Kelly Talbot, and technical editors, Shahla Pirnia and Rae Baker, who performed amazing feats in guiding us to improve this book.

We also owe a debt of gratitude to our literary agent, Carole Jelen of Waterside Productions, for continuing to assist in nailing down these projects. Thanks for all your hard work herding us authors.

We also want to express our condolences to the family and friends of Darril Gibson. Darril, you are missed.

—Mike and Michael

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. 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 over the years.

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 for continuing your excellent contribution 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: every year is another wonderful experience with you. To Slayde and Remi: always remember that you are loved no matter where you go or what you become. 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: I've heard that when you make a sandwich, it's called a peanut butter and banana "Hunka Hunka Burning Lunch"!

—James Michael Stewart

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 the author of more than 200 books and video courses, including the companion book to this study guide: *CISSP Official*

ISC2 Practice Tests, the *CompTIA CySA+ Study Guide*, the *CompTIA Security+ (SY0-701) Study Guide*, and *Cyberwarfare: Information Operations in a Connected World*. Mike offers study groups for the CISSP, SSCP, CCSP, Security+, and other major certifications on his website at www.certmike.com.



James Michael Stewart, CISSP, CEH, CHFI, ECSA, CND, ECIH, CySA+, PenTest+, CASP+, Security+, Network+, A+, CTT+, CEI, and CFR, has been writing and training for more than 25 years, with a 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 80 books on security certification, Microsoft topics, and network administration. Michael is the author of the official online

virtual lab sets for CompTIA's Security+, CASP+, and PenTest+, as well as hundreds of other labs focusing on Microsoft Windows, Linux, internet, and security concepts. More information about Michael can be found at his website at www.impactonline.com.

Darril Gibson, CISSP (1958–2022), was the CEO of YCDA, LLC and regularly wrote and consulted on a wide variety of technical and security topics and held numerous other certifications, including MCSE, MCDBA, MCSA, MCITP, ITIL v3, and Security+. He authored or coauthored more than 30 books, including multiple prior editions of the *CISSP Study Guide*. Darril was greatly respected in the cybersecurity, training, and education fields and will be missed.

About the Technical Editors

Rae Baker is a senior open source intelligence analyst, public speaker, licensed private investigator, and Wiley author specializing in maritime intelligence and OSINT training. She is the owner of OSINT training company Kase Scenarios and she holds several prominent industry certificates, including SANS GOSI and Associate of ISC2 (CISSP). More information about Rae can be found at <http://raebaker.net>.

Shahla Pirnia is a freelance technical editor and proofreader with a focus on cybersecurity and certification topics. She currently serves as a technical editor for CertMike.com. Shahla earned BS degrees in computer and information science and psychology from the University of Maryland Global Campus and an Associate of Arts in information systems from Montgomery College, Maryland. Shahla's IT certifications include CompTIA Security+, Network+, A+, and ISC2 CC.

Contents at a Glance

<i>Introduction</i>		<i>xxxv</i>
<i>Assessment Test</i>		<i>lx</i>
Chapter 1	Security Governance Through Principles and Policies	1
Chapter 2	Personnel Security and Risk Management Concepts	49
Chapter 3	Business Continuity Planning	121
Chapter 4	Laws, Regulations, and Compliance	151
Chapter 5	Protecting Security of Assets	189
Chapter 6	Cryptography and Symmetric Key Algorithms	227
Chapter 7	PKI and Cryptographic Applications	271
Chapter 8	Principles of Security Models, Design, and Capabilities	317
Chapter 9	Security Vulnerabilities, Threats, and Countermeasures	359
Chapter 10	Physical Security Requirements	443
Chapter 11	Secure Network Architecture and Components	491
Chapter 12	Secure Communications and Network Attacks	581
Chapter 13	Managing Identity and Authentication	641
Chapter 14	Controlling and Monitoring Access	681
Chapter 15	Security Assessment and Testing	727
Chapter 16	Managing Security Operations	769
Chapter 17	Preventing and Responding to Incidents	809
Chapter 18	Disaster Recovery Planning	869
Chapter 19	Investigations and Ethics	919
Chapter 20	Software Development Security	951
Chapter 21	Malicious Code and Application Attacks	1005
Appendix A	Answers to Review Questions	1055
Appendix B	Answers to Written Labs	1115
<i>Index</i>		<i>1133</i>

Contents

<i>Introduction</i>	<i>xxxv</i>
<i>Assessment Test</i>	<i>lx</i>
Chapter 1	Security Governance Through Principles and Policies 1
Security 101	3
Understand and Apply Security Concepts	4
Confidentiality	5
Integrity	6
Availability	6
DAD, Overprotection, Authenticity, Nonrepudiation, and AAA Services	7
Protection Mechanisms	11
Security Boundaries	13
Evaluate and Apply Security Governance Principles	14
Third-Party Governance	15
Documentation Review	16
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	27
Security Policy, Standards, Procedures, and Guidelines	27
Security Policies	28
Security Standards, Baselines, and Guidelines	28
Security Procedures	29
Threat Modeling	29
Identifying Threats	30
Determining and Diagramming Potential Attacks	32
Performing Reduction Analysis	33
Prioritization and Response	33
Supply Chain Risk Management	35
Summary	38
Study Essentials	39
Written Lab	41
Review Questions	42

Chapter 2	Personnel Security and Risk Management Concepts	49
	Personnel Security Policies and Procedures	51
	Job Descriptions and Responsibilities	51
	Candidate Screening and Hiring	52
	Onboarding: Employment Agreements and Policy-Driven Requirements	53
	Employee Oversight	55
	Offboarding, Transfers, and Termination Processes	56
	Vendor, Consultant, and Contractor Agreements and Controls	58
	Understand and Apply Risk Management Concepts	60
	Risk Terminology and Concepts	61
	Asset Valuation	64
	Identify Threats and Vulnerabilities	65
	Risk Assessment/Analysis	66
	Risk Responses	73
	Cybersecurity Insurance	75
	Cost vs. Benefit of Security Controls	76
	Countermeasure Selection and Implementation	80
	Applicable Types of Controls	82
	Security Control Assessment	84
	Monitoring and Measurement	84
	Risk Reporting and Documentation	85
	Continuous Improvement	86
	Legacy Risk	87
	Risk Frameworks	87
	Social Engineering	90
	Social Engineering Principles	92
	Eliciting Information	94
	Prepending	94
	Phishing	95
	Spear Phishing	97
	Whaling	97
	Spam	98
	Shoulder Surfing	99
	Invoice Scams	99
	Hoax	100
	Impersonation and Masquerading	100
	Tailgating and Piggybacking	100
	Dumpster Diving	102
	Identity Fraud	102
	Typosquatting	103
	Influence Campaigns	104

Establish and Maintain a Security Awareness, Education, and Training Program	106
Awareness	106
Training	107
Education	107
Improvements	108
Effectiveness Evaluation	109
Summary	110
Study Essentials	111
Written Lab	114
Review Questions	115

Chapter 3 Business Continuity Planning 121

Planning for Business Continuity	122
Project Scope and Planning	123
Organizational Review	124
BCP Team Selection	125
Resource Requirements	127
External Dependencies	128
Business Impact Analysis	131
Identifying Priorities	132
Risk Identification	133
Likelihood Assessment	134
Impact Analysis	135
Resource Prioritization	137
Continuity Planning	137
Strategy Development	138
Provisions and Processes	138
Plan Approval and Implementation	140
Plan Approval	140
Plan Implementation	140
Communication, Training and Education	141
BCP Documentation	141
Summary	145
Study Essentials	145
Written Lab	146
Review Questions	147

Chapter 4 Laws, Regulations, and Compliance 151

Categories of Laws	152
Criminal Law	152
Civil Law	154
Administrative Law	154

	Laws	155
	Computer Crime	155
	Intellectual Property (IP)	160
	Software Licensing	166
	Import/Export	167
	Privacy	168
	State Privacy Laws	179
	Compliance	179
	Contracting and Procurement	181
	Summary	182
	Study Essentials	182
	Written Lab	184
	Review Questions	185
Chapter 5	Protecting Security of Assets	189
	Identifying and Classifying Information and Assets	190
	Defining Sensitive Data	190
	Defining Data Classifications	192
	Defining Asset Classifications	195
	Understanding Data States	195
	Determining Compliance Requirements	196
	Determining Data Security Controls	197
	Establishing Information and Asset Handling Requirements	198
	Data Maintenance	199
	Data Loss Prevention	199
	Labeling Sensitive Data and Assets	200
	Handling Sensitive Information and Assets	202
	Data Collection Limitation	202
	Data Location	203
	Storing Sensitive Data	203
	Data Destruction	204
	Ensuring Appropriate Data and Asset Retention	207
	Data Protection Methods	208
	Digital Rights Management	209
	Cloud Access Security Broker	210
	Pseudonymization	210
	Tokenization	211
	Anonymization	212
	Understanding Data Roles	214
	Data Owners	214
	Data Controllers and Processors	215
	Data Custodians	216
	Users and Subjects	216

	Using Security Baselines	216
	Comparing Tailoring and Scoping	217
	Standards Selection	218
	Summary	219
	Study Essentials	220
	Written Lab	221
	Review Questions	222
Chapter 6	Cryptography and Symmetric Key Algorithms	227
	Cryptographic Foundations	228
	Goals of Cryptography	228
	Cryptography Concepts	231
	Cryptographic Mathematics	232
	Ciphers	239
	Modern Cryptography	246
	Cryptographic Keys	246
	Symmetric Key Algorithms	248
	Asymmetric Key Algorithms	250
	Hashing Algorithms	253
	Symmetric Cryptography	253
	Block Cipher Modes of Operation	254
	Data Encryption Standard	256
	Triple DES	256
	International Data Encryption Algorithm	257
	Blowfish	258
	SKIPJACK	258
	Rivest Ciphers	258
	Advanced Encryption Standard	259
	CAST	260
	Comparison of Symmetric Encryption Algorithms	260
	Symmetric Key Management	261
	Cryptographic Life Cycle	263
	Summary	264
	Study Essentials	264
	Written Lab	266
	Review Questions	267
Chapter 7	PKI and Cryptographic Applications	271
	Asymmetric Cryptography	272
	Public and Private Keys	272
	RSA	274
	ElGamal	275

Elliptic Curve Cryptography	276
Diffie–Hellman Key Exchange	277
Quantum Cryptography	278
Hash Functions	279
SHA Family	280
MD5	281
RIPEMD	282
Comparison of Hash Function Value Lengths	282
Digital Signatures	283
HMAC	284
Digital Signature Standard	285
Public Key Infrastructure	286
Certificates	286
Certificate Authorities	287
Certificate Life Cycle	288
Certificate Formats	291
Asymmetric Key Management	292
Hybrid Cryptography	293
Applied Cryptography	294
Portable Devices	294
Email	295
Web Applications	298
Steganography and Watermarking	300
Networking	302
Emerging Applications	304
Cryptographic Attacks	306
Summary	309
Study Essentials	310
Written Lab	311
Review Questions	312
Chapter 8	
Principles of Security Models, Design, and Capabilities	317
Secure Design Principles	319
Objects and Subjects	319
Closed and Open Systems	321
Secure Defaults	322
Fail Securely	323
Keep It Simple and Small	325
Zero-Trust	326
Trust but Verify	328
Privacy by Design	328
Secure Access Service Edge (SASE)	329

Techniques for Ensuring CIA	330
Confinement	330
Bounds	330
Isolation	331
Access Controls	331
Trust and Assurance	331
Understand the Fundamental Concepts of Security Models	332
Trusted Computing Base	333
State Machine Model	334
Information Flow Model	335
Noninterference Model	335
Composition Theories	336
Take-Grant Model	336
Access Control Matrix	337
Bell–LaPadula Model	338
Biba Model	340
Clark–Wilson Model	342
Brewer and Nash Model	343
Select Controls Based on Systems Security Requirements	345
Common Criteria	345
Authorization to Operate	348
Understand Security Capabilities of Information Systems	349
Memory Protection	349
Virtualization	349
Trusted Platform Module (TPM)	349
Interfaces	350
Fault Tolerance	350
Encryption/Decryption	350
Manage the Information System Life Cycle	350
Summary	352
Study Essentials	353
Written Lab	354
Review Questions	355

Chapter 9	Security Vulnerabilities, Threats, and Countermeasures	359
	Shared Responsibility	360
	Data Localization and Data Sovereignty	362
	Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements	363
	Hardware	364
	Firmware	377

Client-Based Systems	378
Mobile Code	379
Local Caches	381
Server-Based Systems	381
Large-Scale Parallel Data Systems	382
Grid Computing	383
Peer to Peer	384
Industrial Control Systems	384
Distributed Systems	386
High-Performance Computing (HPC) Systems	387
Real-Time Operating Systems	388
Internet of Things	389
Edge and Fog Computing	390
Embedded Devices and Cyber-Physical Systems	391
Static Systems	392
Cyber-Physical Systems	393
Security Concerns of Embedded and Static Systems	393
Microservices	396
Infrastructure as Code	397
Immutable Architecture	398
Virtualized Systems	399
Virtual Software	401
Virtualized Networking	402
Software-Defined Everything	402
Virtualization Security Management	404
Containerization	406
Mobile Devices	407
Mobile Device Security Features	408
Mobile Device Deployment Policies	419
Essential Security Protection Mechanisms	424
Process Isolation	425
Hardware Segmentation	425
Root of Trust	426
System Security Policy	426
Common Security Architecture Flaws and Issues	427
Covert Channels	427
Attacks Based on Design or Coding Flaws	428
Rootkits	429
Incremental Attacks	430
Summary	431
Study Essentials	432
Written Lab	436
Review Questions	437

Chapter 10	Physical Security Requirements	443
	Apply Security Principles to Site and Facility Design	444
	Secure Facility Plan	444
	Site Selection	445
	Facility Design	446
	Implement Site and Facility Security Controls	449
	Equipment Failure	450
	Wiring Closets	450
	Server Rooms/Data Centers	452
	Intrusion Detection Systems	454
	Cameras	458
	Access Abuses	459
	Media Storage Facilities	459
	Evidence Storage	460
	Work Area Security	461
	Utility Considerations	462
	Fire Prevention, Detection, and Suppression	467
	Implement and Manage Physical Security	473
	Perimeter Security Controls	474
	Internal Security Controls	478
	Key Performance Indicators of Physical Security	479
	Summary	480
	Study Essentials	481
	Written Lab	484
	Review Questions	485
Chapter 11	Secure Network Architecture and Components	491
	OSI Model	493
	History of the OSI Model	493
	OSI Functionality	494
	Encapsulation/Deencapsulation	494
	OSI Layers	496
	TCP/IP Model	501
	Analyzing Network Traffic	502
	Common Application Layer Protocols	503
	Transport Layer Protocols	504
	Domain Name System	506
	DNS Poisoning	508
	Domain Hijacking	511
	Internet Protocol (IP) Networking	512
	IPv4 vs. IPv6	513
	IP Classes	514

ICMP	516
IGMP	516
ARP Concerns	516
Secure Communication Protocols	517
Implications of Multilayer Protocols	518
Converged Protocols	520
Voice over Internet Protocol (VoIP)	521
Software-Defined Networking	522
Segmentation	523
Edge Networks	526
Wireless Networks	527
Securing the SSID	528
Wireless Channels	529
Conducting a Site Survey	530
Wireless Security	530
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
Satellite Communications	543
Cellular Networks	544
Content Distribution Networks (CDNs)	544
Secure Network Components	545
Secure Operation of Hardware	546
Common Network Equipment	547
Network Access Control	549
Firewalls	551
Endpoint Security	556
Cabling, Topology, and Transmission Media Technology	559
Transmission Media	560
Transport Architecture	564
Network Topologies	565
Ethernet	568
Sub-Technologies	568
Summary	572
Study Essentials	573
Written Lab	575
Review Questions	576

Chapter 12	Secure Communications and Network Attacks	581
	Protocol Security Mechanisms	582
	Authentication Protocols	582
	Port Security	585
	Quality of Service (QoS)	585
	Secure Voice Communications	587
	Public Switched Telephone Network	587
	Voice over Internet Protocol (VoIP)	587
	Vishing and Phreaking	589
	PBX Fraud and Abuse	590
	Remote Access Security Management	591
	Remote Access and Telecommuting Techniques	592
	Remote Connection Security	592
	Plan a Remote Access Security Policy	593
	Network Administrative Functions	594
	Multimedia Collaboration	595
	Remote Meeting	595
	Instant Messaging and Chat	596
	Monitoring and Management	597
	Load Balancing	597
	Virtual IP Addresses	599
	Active-Active vs. Active-Passive	599
	Manage Email Security	600
	Email Security Goals	601
	Understand Email Security Issues	602
	Email Security Solutions	603
	Virtual Private Network	606
	Tunneling	606
	How VPNs Work	607
	Always-On	610
	Split Tunnel vs. Full Tunnel	610
	Common VPN Protocols	611
	Switching and Virtual LANs	613
	MAC Flooding Attack	616
	MAC Cloning	617
	Network Address Translation	617
	Private IP Addresses	620
	Stateful NAT	621
	Automatic Private IP Addressing	621
	Third-Party Connectivity	622
	Switching Technologies	624
	Circuit Switching	624

	Packet Switching	625
	Virtual Circuits	626
	WAN Technologies	626
	Fiber-Optic Links	629
	Prevent or Mitigate Network Attacks	630
	Eavesdropping	630
	Modification Attacks	630
	Summary	631
	Study Essentials	632
	Written Lab	635
	Review Questions	636
Chapter 13	Managing Identity and Authentication	641
	Controlling Access to Assets	643
	Controlling Physical and Logical Access	644
	The CIA Triad and Access Controls	644
	The AAA Model	645
	Identification and Authentication Strategy	645
	Comparing Subjects and Objects	646
	Registration, Proofing, and Establishment of Identity	647
	Authorization and Accounting	648
	Authentication Factors Overview	649
	Something You Know	651
	Something You Have	654
	Something You Are	656
	Multifactor Authentication (MFA)	659
	Passwordless Authentication	660
	Device Authentication	661
	Service Authentication	661
	Mutual Authentication	662
	Implementing Identity Management	662
	Single Sign-On	663
	SSO and Federated Identities	664
	Credential Management Systems	666
	Credential Manager Apps	666
	Scripted Access	667
	Session Management	667
	Managing the Identity and Access Provisioning Life Cycle	668
	Provisioning and Onboarding	668
	Deprovisioning and Offboarding	670
	Role Definition and Transition	670
	Account Maintenance	671
	Account Access Review	671

	Summary	672
	Study Essentials	672
	Written Lab	675
	Review Questions	676
Chapter 14	Controlling and Monitoring Access	681
	Comparing Access Control Models	682
	Comparing Permissions, Rights, and Privileges	682
	Understanding Authorization Mechanisms	683
	Defining Requirements with a Security Policy	685
	Introducing Access Control Models	685
	Discretionary Access Control	686
	Nondiscretionary Access Controls	687
	Implementing Authentication Systems	694
	Implementing SSO on the Internet	694
	Implementing SSO on Internal Networks	698
	Zero-Trust Access Policy Enforcement	702
	Understanding Access Control Attacks	703
	Risk Elements	704
	Common Access Control Attacks	704
	Core Protection Methods	717
	Summary	719
	Study Essentials	720
	Written Lab	721
	Review Questions	722
Chapter 15	Security Assessment and Testing	727
	Building a Security Assessment and Testing Program	729
	Security Testing	729
	Security Assessments	731
	Security Audits	732
	Performing Vulnerability Assessments	735
	Describing Vulnerabilities	736
	Vulnerability Scans	736
	Penetration Testing	747
	Compliance Checks	750
	Testing Your Software	750
	Code Review and Testing	751
	Interface Testing	755
	Misuse Case Testing	756
	Test Coverage Analysis	757
	Website Monitoring	757
	Training and Exercises	758

	Implementing Security Management Processes and Collecting Security Process Data	759
	Log Reviews	759
	Account Management	760
	Disaster Recovery and Business Continuity	761
	Training and Awareness	761
	Key Performance and Risk Indicators	762
	Summary	762
	Exam Essentials	763
	Written Lab	764
	Review Questions	765
Chapter 16	Managing Security Operations	769
	Apply Foundational Security Operations Concepts	771
	Need-to-Know and Least Privilege	772
	Segregation of Duties (SoD) and Responsibilities	773
	Two-Person Control	774
	Job Rotation	775
	Mandatory Vacations	775
	Privileged Account Management	775
	Service-Level Agreements (SLAs)	777
	Address Personnel Safety and Security	778
	Duress	778
	Travel	778
	Emergency Management	779
	Security Training and Awareness	780
	Provision Information and Assets Securely	780
	Information and Asset Ownership	781
	Asset Management	781
	Apply Resource Protection	783
	Media Management	783
	Media Protection Techniques	783
	Managed Services in the Cloud	786
	Shared Responsibility with Cloud Service Models	787
	Scalability and Elasticity	789
	Serverless Architecture	790
	Perform Configuration Management (CM)	790
	Provisioning	791
	Baselining	791
	Using Images for Baselining	791
	Automation	792