

(ISC)²[®]



CISSP[®]

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



SYBEX
A Wiley Brand

Table of Contents

[Cover](#)

[Title Page](#)

[Copyright](#)

[Dedication](#)

[Acknowledgments](#)

[About the Authors](#)

[About the Technical Editors](#)

[Foreword](#)

[Introduction](#)

[Overview of the CISSP Exam](#)

[The Elements of This Study Guide](#)

[Interactive Online Learning Environment and TestBank](#)

[Study Guide Exam Objectives](#)

[Objective Map](#)

[Reader Support for This Book](#)

[Assessment Test](#)

[Answers to Assessment Test](#)

[Chapter 1: Security Governance Through Principles and Policies](#)

[Security 101](#)

[Understand and Apply Security Concepts](#)

[Security Boundaries](#)

[Evaluate and Apply Security Governance Principles](#)

[Manage the Security Function](#)

[Security Policy, Standards, Procedures, and Guidelines](#)

[Threat Modeling](#)

[Supply Chain Risk Management](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

[Chapter 2: Personnel Security and Risk Management Concepts](#)

[Personnel Security Policies and Procedures](#)

[Understand and Apply Risk Management Concepts](#)

[Social Engineering](#)

[Establish and Maintain a Security Awareness, Education, and Training Program](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

[Chapter 3: Business Continuity Planning](#)

[Planning for Business Continuity](#)

[Project Scope and Planning](#)

[Business Impact Analysis](#)

[Continuity Planning](#)

[Plan Approval and Implementation](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

Chapter 4: Laws, Regulations, and Compliance

Categories of Laws

Laws

State Privacy Laws

Compliance

Contracting and Procurement

Summary

Exam Essentials

Written Lab

Review Questions

Chapter 5: Protecting Security of Assets

Identifying and Classifying Information and Assets

Establishing Information and Asset Handling Requirements

Data Protection Methods

Understanding Data Roles

Using Security Baselines

Summary

Exam Essentials

Written Lab

Review Questions

Chapter 6: Cryptography and Symmetric Key Algorithms

Cryptographic Foundations

Modern Cryptography

Symmetric Cryptography

Cryptographic Lifecycle

Summary

Exam Essentials

[Written Lab](#)

[Review Questions](#)

[Chapter 7: PKI and Cryptographic Applications](#)

[Asymmetric Cryptography](#)

[Hash Functions](#)

[Digital Signatures](#)

[Public Key Infrastructure](#)

[Asymmetric Key Management](#)

[Hybrid Cryptography](#)

[Applied Cryptography](#)

[Cryptographic Attacks](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

[Chapter 8: Principles of Security Models, Design, and Capabilities](#)

[Secure Design Principles](#)

[Techniques for Ensuring CIA](#)

[Understand the Fundamental Concepts of Security Models](#)

[Select Controls Based on Systems Security Requirements](#)

[Understand Security Capabilities of Information Systems](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

Chapter 9: Security Vulnerabilities, Threats, and Countermeasures

Shared Responsibility

Assess and Mitigate the Vulnerabilities of Security Architectures, Designs, and Solution Elements

Client-Based Systems

Server-Based Systems

Industrial Control Systems

Distributed Systems

High-Performance Computing (HPC) Systems

Internet of Things

Edge and Fog Computing

Embedded Devices and Cyber-Physical Systems

Specialized Devices

Microservices

Infrastructure as Code

Virtualized Systems

Containerization

Serverless Architecture

Mobile Devices

Essential Security Protection Mechanisms

Common Security Architecture Flaws and Issues

Summary

Exam Essentials

Written Lab

Review Questions

Chapter 10: Physical Security Requirements

Apply Security Principles to Site and Facility Design

Implement Site and Facility Security Controls

[Implement and Manage Physical Security](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

[Chapter 11: Secure Network Architecture and Components](#)

[OSI Model](#)

[TCP/IP Model](#)

[Analyzing Network Traffic](#)

[Common Application Layer Protocols](#)

[Transport Layer Protocols](#)

[Domain Name System](#)

[Internet Protocol \(IP\) Networking](#)

[ARP Concerns](#)

[Secure Communication Protocols](#)

[Implications of Multilayer Protocols](#)

[Microsegmentation](#)

[Wireless Networks](#)

[Other Communication Protocols](#)

[Cellular Networks](#)

[Content Distribution Networks \(CDNs\)](#)

[Secure Network Components](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

[Chapter 12: Secure Communications and Network Attacks](#)

[Protocol Security Mechanisms](#)

[Secure Voice Communications](#)

[Remote Access Security Management](#)

[Multimedia Collaboration](#)

[Load Balancing](#)

[Manage Email Security](#)

[Virtual Private Network](#)

[Switching and Virtual LANs](#)

[Network Address Translation](#)

[Third-Party Connectivity](#)

[Switching Technologies](#)

[WAN Technologies](#)

[Fiber-Optic Links](#)

[Security Control Characteristics](#)

[Prevent or Mitigate Network Attacks](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

[Chapter 13: Managing Identity and Authentication](#)

[Controlling Access to Assets](#)

[Managing Identification and Authentication](#)

[Implementing Identity Management](#)

[Managing the Identity and Access Provisioning Lifecycle](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

[Chapter 14: Controlling and Monitoring Access](#)

[Comparing Access Control Models](#)

[Implementing Authentication Systems](#)

[Understanding Access Control Attacks](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

[Chapter 15: Security Assessment and Testing](#)

[Building a Security Assessment and Testing Program](#)

[Performing Vulnerability Assessments](#)

[Testing Your Software](#)

[Implementing Security Management Processes](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

[Chapter 16: Managing Security Operations](#)

[Apply Foundational Security Operations Concepts](#)

[Addressing Personnel Safety and Security](#)

[Provision Resources Securely](#)

[Apply Resource Protection](#)

[Managed Services in the Cloud](#)

[Perform Configuration Management \(CM\)](#)

[Managing Change](#)

[Managing Patches and Reducing Vulnerabilities](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

[Chapter 17: Preventing and Responding to Incidents](#)

[Conducting Incident Management](#)

[Implementing Detective and Preventive Measures](#)

[Logging and Monitoring](#)

[Automating Incident Response](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

[Chapter 18: Disaster Recovery Planning](#)

[The Nature of Disaster](#)

[Understand System Resilience, High Availability, and Fault Tolerance](#)

[Recovery Strategy](#)

[Recovery Plan Development](#)

[Training, Awareness, and Documentation](#)

[Testing and Maintenance](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

[Chapter 19: Investigations and Ethics](#)

[Investigations](#)

[Major Categories of Computer Crime](#)

[Ethics](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

[Chapter 20: Software Development Security](#)

[Introducing Systems Development Controls](#)

[Establishing Databases and Data Warehousing](#)

[Storage Threats](#)

[Understanding Knowledge-Based Systems](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

[Chapter 21: Malicious Code and Application Attacks](#)

[Malware](#)

[Malware Prevention](#)

[Application Attacks](#)

[Injection Vulnerabilities](#)

[Exploiting Authorization Vulnerabilities](#)

[Exploiting Web Application Vulnerabilities](#)

[Application Security Controls](#)

[Secure Coding Practices](#)

[Summary](#)

[Exam Essentials](#)

[Written Lab](#)

[Review Questions](#)

[Appendix A: Answers to Review Questions](#)

[Chapter 1: Security Governance Through Principles and Policies](#)

[Chapter 2: Personnel Security and Risk Management Concepts](#)

[Chapter 3: Business Continuity Planning](#)

[Chapter 4: Laws, Regulations, and Compliance](#)

[Chapter 5: Protecting Security of Assets](#)

[Chapter 6: Cryptography and Symmetric Key Algorithms](#)

[Chapter 7: PKI and Cryptographic Applications](#)

[Chapter 8: Principles of Security Models, Design, and Capabilities](#)

[Chapter 9: Security Vulnerabilities, Threats, and Countermeasures](#)

[Chapter 10: Physical Security Requirements](#)

[Chapter 11: Secure Network Architecture and Components](#)

[Chapter 12: Secure Communications and Network Attacks](#)

[Chapter 13: Managing Identity and Authentication](#)

[Chapter 14: Controlling and Monitoring Access](#)

[Chapter 15: Security Assessment and Testing](#)

[Chapter 16: Managing Security Operations](#)

[Chapter 17: Preventing and Responding to Incidents](#)

[Chapter 18: Disaster Recovery Planning](#)

[Chapter 19: Investigations and Ethics](#)

[Chapter 20: Software Development Security](#)

[Chapter 21: Malicious Code and Application Attacks](#)

[Appendix B: Answers to Written Labs](#)

[Chapter 1: Security Governance Through Principles and Policies](#)

[Chapter 2: Personnel Security and Risk Management Concepts](#)

[Chapter 3: Business Continuity Planning](#)

[Chapter 4: Laws, Regulations, and Compliance](#)

[Chapter 5: Protecting Security of Assets](#)

[Chapter 6: Cryptography and Symmetric Key Algorithms](#)

[Chapter 7: PKI and Cryptographic Applications](#)

[Chapter 8: Principles of Security Models, Design, and Capabilities](#)

[Chapter 9: Security Vulnerabilities, Threats, and Countermeasures](#)

[Chapter 10: Physical Security Requirements](#)

[Chapter 11: Secure Network Architecture and Components](#)

[Chapter 12: Secure Communications and Network Attacks](#)

[Chapter 13: Managing Identity and Authentication](#)

[Chapter 14: Controlling and Monitoring Access](#)

[Chapter 15: Security Assessment and Testing](#)

[Chapter 16: Managing Security Operations](#)

[Chapter 17: Preventing and Responding to Incidents](#)

[Chapter 18: Disaster Recovery Planning](#)

[Chapter 19: Investigations and Ethics](#)

[Chapter 20: Software Development Security](#)

[Chapter 21: Malicious Code and Application Attacks](#)

[Index](#)

[End User License Agreement](#)

List of Tables

Chapter 2

[TABLE 2.1 Comparison of quantitative and qualitative risk analysis](#)

[TABLE 2.2 Quantitative risk analysis formulas](#)

Chapter 5

[TABLE 5.1 Securing email data](#)

[TABLE 5.2 Unmodified data within a database](#)

[TABLE 5.3 Masked data](#)

Chapter 6

[TABLE 6.1 AND operation truth table](#)

[TABLE 6.2 OR operation truth table](#)

[TABLE 6.3 NOT operation truth table](#)

[TABLE 6.4 Exclusive OR operation truth table](#)

[TABLE 6.5 Using the Vigenère system](#)

[TABLE 6.6 The encryption operation](#)

[TABLE 6.7 Symmetric and asymmetric key comparison](#)

[TABLE 6.8 Comparison of symmetric and asymmetric cryptography systems](#)

[TABLE 6.9 Symmetric encryption memorization chart](#)

Chapter 7

[TABLE 7.1 Hash algorithm memorization chart](#)

[TABLE 7.2 Digital certificate formats](#)

Chapter 8

[TABLE 8.1 Subjects and objects](#)

[TABLE 8.2 Fail terms definitions related to physical and digital products](#)

[TABLE 8.3 An access control matrix](#)

[TABLE 8.4 Common Criteria evaluation assurance levels](#)

Chapter 10

[TABLE 10.1 Static voltage and damage](#)

[TABLE 10.2 Fire extinguisher classes](#)

Chapter 11

[TABLE 11.1 IP classes](#)

[TABLE 11.2 IP classes' default subnet masks](#)

[TABLE 11.3 802.11 wireless networking amendments](#)

[TABLE 11.4 UTP categories](#)

Chapter 12

[TABLE 12.1 Common load-balancing scheduling techniques](#)

[TABLE 12.2 Circuit switching vs. packet switching](#)

[TABLE 12.3 Bandwidth levels of SDH and SONET](#)

List of Illustrations

Chapter 1

[FIGURE 1.1 The CIA Triad](#)

[FIGURE 1.2 The five elements of AAA services](#)

[FIGURE 1.3 Strategic, tactical, and operational plan timeline comparison](#)

[FIGURE 1.4 An example of diagramming to reveal threat concerns](#)

[FIGURE 1.5 A risk matrix or risk heat map](#)

Chapter 2

[FIGURE 2.1 Ex-employees must return all company property.](#)

[FIGURE 2.2 The cyclical relationships of risk elements](#)

[FIGURE 2.3 The six major elements of quantitative risk analysis](#)

[FIGURE 2.4 The categories of security controls in a defense-in-depth impleme...](#)

[FIGURE 2.5 The elements of the risk management framework \(RMF\)_\(from NIST SP...](#)

Chapter 3

[FIGURE 3.1 Earthquake hazard map of the United States](#)

Chapter 5

[FIGURE 5.1 Data classifications](#)

[FIGURE 5.2 Clearing a hard drive](#)

Chapter 6

[FIGURE 6.1 Challenge-response authentication protocol](#)

[FIGURE 6.2 The magic door](#)

[FIGURE 6.3 Symmetric key cryptography](#)

[FIGURE 6.4 Asymmetric key cryptography](#)

Chapter 7

[FIGURE 7.1 Asymmetric key cryptography](#)

[FIGURE 7.2 Steganography tool](#)

[FIGURE 7.3 Image with embedded message](#)

Chapter 8

[FIGURE 8.1 Transitive trust](#)

[FIGURE 8.2 The TCB, security perimeter, and reference monitor](#)

[FIGURE 8.3 The take-grant model's directed graph](#)

[FIGURE 8.4 The Bell-LaPadula model](#)

[FIGURE 8.5 The Biba model](#)

[FIGURE 8.6 Memorizing Bell-LaPadula and Biba](#)

[FIGURE 8.7 The Clark-Wilson model](#)

Chapter 9

[FIGURE 9.1 The four-layer protection ring model](#)

[FIGURE 9.2 The lifecycle of an executed process](#)

[FIGURE 9.3 Types of hypervisors](#)

[FIGURE 9.4 Application containers versus a hypervisor](#)

Chapter 10

[FIGURE 10.1 A smartcard's ISO 7816 interface](#)

[FIGURE 10.2 Hot and cold aisles](#)

[FIGURE 10.3 The fire triangle](#)

[FIGURE 10.4 The four primary stages of fire](#)

[FIGURE 10.5 A secure physical boundary with an access control vestibule and ...](#)

Chapter 11

[FIGURE 11.1 The OSI model](#)

[FIGURE 11.2 OSI model encapsulation](#)

[FIGURE 11.3 The OSI model peer layer logical channels](#)

[FIGURE 11.4 OSI model layer-based network container names](#)

[FIGURE 11.5 Comparing the OSI model with the TCP/IP model](#)

[FIGURE 11.6 The TCP three-way handshake](#)

[FIGURE 11.7 An RFID antenna](#)

[FIGURE 11.8 The configuration dialog boxes for a transparent \(left\) vs. a no...](#)

[FIGURE 11.9 A ring topology.](#)

[FIGURE 11.10 A linear bus topology and a tree bus topology.](#)

[FIGURE 11.11 A star topology.](#)

[FIGURE 11.12 A mesh topology.](#)

Chapter 12

[FIGURE 12.1 IPsec's encryption of a packet in transport mode](#)

[FIGURE 12.2 IPsec's encryption of a packet in tunnel mode](#)

[FIGURE 12.3 Two LANs being connected using a tunnel-mode VPN across the inte...](#)

[FIGURE 12.4 A client connecting to a network via a remote-access/tunnel VPN ...](#)

Chapter 13

[FIGURE 13.1 Graph of FRR and FAR errors indicating the CER point](#)

Chapter 14

[FIGURE 14.1 Role-Based Access Control](#)

[FIGURE 14.2 A representation of the boundaries provided by lattice-based acc...](#)

[FIGURE 14.3 Wireshark capture](#)

Chapter 15

[FIGURE 15.1 Nmap scan of a web server run from a Linux system](#)

[FIGURE 15.2 Default Apache server page running on the server scanned in Figu...](#)

[FIGURE 15.3 Nmap scan of a large network run from a Mac system using the Ter...](#)

[FIGURE 15.4 Network vulnerability scan of the same web server that was port ...](#)

[FIGURE 15.5 Web application vulnerability scan of the same web server that w...](#)

[FIGURE 15.6 Scanning a database-backed application with sqlmap](#)

[FIGURE 15.7 Penetration testing process](#)

[FIGURE 15.8 The Metasploit Framework automated system exploitation tool allo...](#)

[FIGURE 15.9 Fagan inspections follow a rigid formal process, with defined en...](#)

[FIGURE 15.10 Prefuzzing input file containing a series of 1s](#)

[FIGURE 15.11 The input file from Figure 15.10 after being run through the zz...](#)

Chapter 16

[FIGURE 16.1 Cloud shared responsibility model](#)

[FIGURE 16.2 Creating and deploying images](#)

[FIGURE 16.3 Web server and database server](#)

Chapter 17

[FIGURE 17.1 Incident management](#)

[FIGURE 17.2 SYN flood attack](#)

[FIGURE 17.3 A man-in-the-middle attack](#)

[FIGURE 17.4 Intrusion prevention system](#)

[FIGURE 17.5 Viewing a log entry](#)

Chapter 18

[FIGURE 18.1 Seismic hazard map](#)

[FIGURE 18.2 Flood hazard map for Miami-Dade County, Florida](#)

[FIGURE 18.3 Failover cluster with network load balancing](#)

Chapter 20

[FIGURE 20.1 RStudio Desktop IDE](#)

[FIGURE 20.2 Security vs. user-friendliness vs. functionality](#)

[FIGURE 20.3 The iterative lifecycle model with feedback loop](#)

[FIGURE 20.4 The spiral lifecycle mode](#)

[FIGURE 20.5 Software Assurance Maturity Model](#)

[FIGURE 20.6 The IDEAL model](#)

[FIGURE 20.7 Gantt chart](#)

[FIGURE 20.8 The DevOps model](#)

[FIGURE 20.9 Hierarchical data model](#)

[FIGURE 20.10 Customers table from a relational database](#)

[FIGURE 20.11 ODBC as the interface between applications and a back-end datab...](#)

Chapter 21

[FIGURE 21.1 Account number input page](#)

[FIGURE 21.2 Account information page](#)

[FIGURE 21.3 Account information page after blind SQL injection](#)

[FIGURE 21.4 Account creation page](#)

[FIGURE 21.5 Example web server directory structure](#)

[FIGURE 21.6 Message board post rendered in a browser](#)

[FIGURE 21.7 XSS attack rendered in a browser](#)

[FIGURE 21.8 Web application firewall](#)

[FIGURE 21.9 SQL error disclosure](#)

(ISC)²®
CISSP® Certified
Information Systems
Security Professional

Official Study Guide

Ninth Edition



Mike Chapple
James Michael Stewart
Darril Gibson



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.

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)² and CISSP are trademarks or registered trademarks of (ISC)², 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)² 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.

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.

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 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.