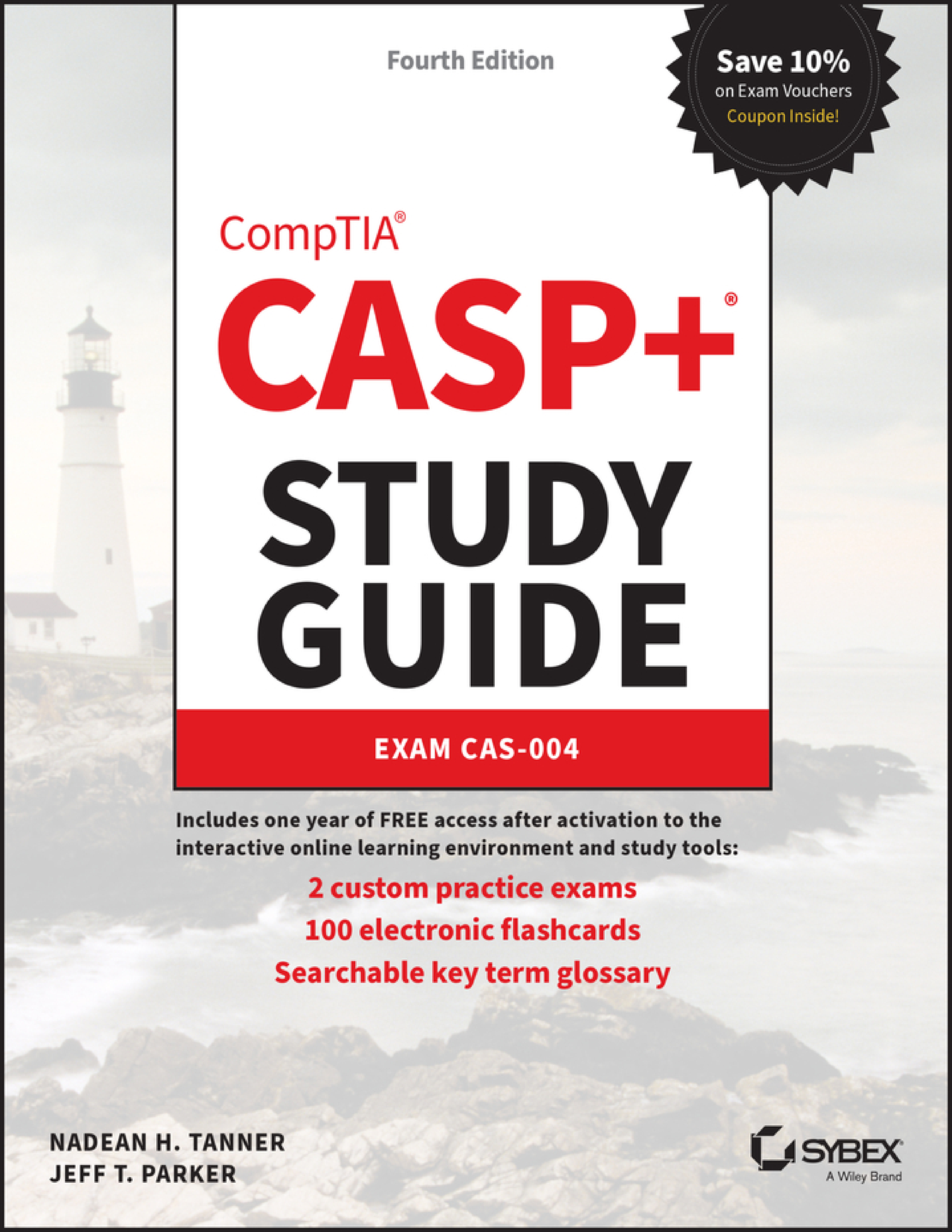

Fourth Edition

CompTIA® CASP+® STUDY GUIDE

EXAM CAS-004

Includes one year of FREE access after activation to the interactive online learning environment and study tools:

2 custom practice exams
100 electronic flashcards
Searchable key term glossary

NADEAN H. TANNER
JEFF T. PARKER

SYBEX
A Wiley Brand

Table of Contents

List of Tables

Chapter 1

Chapter 3

Chapter 6

Chapter 8

Chapter 9

List of Illustrations

Chapter 1

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

CompTIA® CASP+® Study Guide

Exam CAS-004

Fourth Edition

Nadean H. Tanner

Jeff T. Parker

SYBEX®
A Wiley Brand

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

Published simultaneously in Canada and the United Kingdom.

ISBN: 978-1-119-80316-4
ISBN: 978-1-119-80318-8 (ebk.)
ISBN: 978-1-119-80317-1 (ebk.)

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. 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 or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States 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: 2022942942

Cover image: © Jeremy Woodhouse/Getty Images, Inc.
Cover design: Wiley

Acknowledgments

My first three books were dedicated to Kenneth, Shelby, and Gavin: thank you for your love and support and all your electronical advice.

To Kelly Talbot, my editor, thank you for your kind patience and making things easy when you could, which wasn't often.

To Chris Crayton, my technical editor, you were right—most of the time. As a woman in IT for 20+ years, I know there are still man-made disasters.

And to Ophelia…because I can, so I did.

About the Authors

Nadean H. Tanner is the senior manager of consulting at Mandiant, working most recently on building real-world cyber range engagements to practice threat hunting and incident response. She has been in IT for more than 20 years and specifically in cybersecurity for more than a decade. She holds more than 30 industry certifications including CompTIA CASP+, Security+, and (ISC)^2 CISSP.

Tanner has trained and consulted for Fortune 500 companies and the U.S. Department of Defense in cybersecurity, forensics, analysis, red/blue teaming, vulnerability management, and security awareness.

She is the author of the *Cybersecurity Blue Team Toolkit,* published by Wiley in 2019, and *CASP+ Practice Tests: Exam CAS-004*, published by Sybex in 2020. She also was the technical editor for the *CompTIA Security+ Study Guide: Exam SY0-601* and *CompTIA PenTest+ Study Guide: Exam PT0-002* written by Mike Chapple and David Seidl.

In her spare time, Tanner enjoys speaking at technical conferences such as Black Hat, Wild West Hacking Fest, and OWASP events.

Jeff T. Parker is an information security professional with more than 20 years' experience in cybersecurity consulting and IT risk management. Jeff started in information security while working as a software engineer for HP in Boston, Massachusetts. Jeff then took the role of a global IT risk manager for Deutsche Post to enjoy Prague in the Czech Republic with his family for several years. There he developed and oversaw the implementation of a new IT risk management strategy. Today, Jeff most enjoys time with his two children in Nova Scotia. Currently, Jeff is developing custom e-learning courses in security awareness for Mariner Innovations.

Jeff maintains several certifications, including CISSP, CEH, and CompTIA's CySA+ and ITT+. He also coauthored the book *Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework* (Wiley, 2017) with Jessey Bullock. Jeff also has written Wiley practice exam books for the CompTIA certifications CySA+ and the A+ (2018 and 2019, respectively).

About the Technical Editor

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 of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional and teaching awards, and has served as a state-level SkillsUSA final competition judge.

Table of Exercises

Introduction

The CASP+ certification was developed by the Computer Technology Industry Association (CompTIA) to provide an industry-wide means of certifying the competency of security professionals who have a minimum of 10 years' general hands-on IT experience with at least 5 years' hands-on IT security experience. The security professional's job is to protect the confidentiality, integrity, and availability of an organization's valuable information assets. As such, these individuals need to have the ability to apply critical thinking and judgment.

NOTE According to CompTIA, the CASP+ certification is a vendor-neutral credential. CASP+ validates advanced-level security skills and knowledge internationally. There is no prerequisite, but CASP+ certification is intended to follow CompTIA Network+, Security+, CySA+, Cloud+, and PenTest+ or equivalent certifications/experience and has a technical, “hands-on” focus at the enterprise level.

Many certification books present material for you to memorize before the exam, but this book goes a step further in that it offers best practices, tips, and hands-on exercises that help those in the field of security better protect critical assets, build defense in depth, and accurately assess risk.

If you're preparing to take the CASP+ exam, it is a good idea to find out as much information as possible about computer security practices and techniques. Because this test is designed for those with years of experience, you will be better prepared by having the most hands-on experience possible; this study guide was written with this in mind. We have included hands-on exercises, real-world scenarios, and review questions at the end of each chapter to give you some idea as to what the exam is like. You should be able to answer at least 90 percent of the test questions in this book correctly before attempting the exam; if you're unable to do so, reread the problematic chapters and try the questions again. Your score should improve.

Before You Begin the CompTIA CASP+ Certification Exam

Before you begin studying for the exam, it's good for you to know that the CASP+ certification is offered by CompTIA (an industry association responsible for many certifications) and is granted to those who obtain a passing score on a single exam. Before you begin studying for the exam, learn all you can about the certification.

> NOTE A list of the CASP+ CAS-004 exam objectives is presented in this introduction. See the section “The CASP+ Exam Objective Map.”

Obtaining CASP+ certification demonstrates that you can help your organization design and maintain system and network security services to secure the organization's assets. By obtaining CASP+ certification, you show that you have the technical knowledge and skills required to conceptualize, design, and engineer secure solutions across complex enterprise environments.

Who Should Read This Book

The *CompTIA CASP+ Study Guide: Exam CAS-004, Fourth Edition*, is designed to give you insight into the working world of IT security, and it describes the types of tasks and activities that a security professional with 5–10 years of experience carries out. Organized classes and study groups are the ideal structures for obtaining and practicing with the recommended equipment.

> NOTE College classes, training classes, and boot camps are recommended ways to gain proficiency with the tools and techniques discussed in the book. However, nothing delivers hands-on learning like experiencing your own attempts, successes, and mistakes—on a home lab. More on home labs later.

What You Will Learn

This *CompTIA CASP+ Study Guide* covers all you need to know to pass the CASP+ exam. The exam is based on exam objectives, and this study guide is based on the current iteration of the CASP+ exam, version CAS-004.

Per the CASP+ CompTIA objectives for exam version CAS-004, the four domains include the following:

- Domain 1.0 Security Architecture
- Domain 2.0 Security Operations
- Domain 3.0 Security Engineering and Cryptography
- Domain 4.0 Governance, Risk, and Compliance

Each of these four domains further divide into objectives. For example, the fourth domain, “Governance, Risk, and Compliance,” is covered across three objectives:

> 4.1 Given a set of requirements, apply the appropriate risk strategies.
>
> 4.2 Explain the importance of managing and mitigating vendor risk.
>
> 4.3 Explain compliance frameworks and legal considerations, and their organizational impact.
>
> 4.4 Explain the importance of business continuity and disaster recovery concepts.

These objectives read like a job task, but they are more akin to a named subset of knowledge. Many subobjectives and topics are found under each objective. These are listed hierarchically, ranging from 20 to 50 topics per objective. Yes, that's a lot of topics when you add it all up. In short, there is a lot of material to cover. Next, we address how the book tackles it all.

How This Book Is Organized

Remember how we just explained the CASP+ exam is based on domains and objectives? Your goal for exam preparation is essentially to cover all of those subobjectives and topics. That was our goal, too, in writing this study guide, so that's how we structured this book—around the same exam objectives, specifically calling out every subobjective and topic. If a topic or phrase from the exam objectives list isn't specifically called out, the concepts and understanding behind that topic or phrase are discussed thoroughly in the relevant chapters.

Nonetheless, CompTIA didn't structure the exam objectives to make for good reading or an easy flow. It would be simple to tell you that each chapter correlates exactly to two or three objectives. Instead, the book is laid out to create a balance between a relevant flow of information for learning and relatable coverage of the exam objectives. This book structure then serves to be most helpful for identifying and filling any knowledge gaps that you might have in a certain area and, in turn, best prepare you for the exam.

Extra Bits

Beyond what the exam requires, there is of course some “added value” in the form of tips, notes, stories, and URLs where you can go for additional information online. This is typical for the Sybex study guide format. The extra bits are obviously set apart from the study guide text, and they can be enjoyed as you wish. In most cases, URLs will point to a recent news event related to the topic at hand, a link to the cited regulation, or the site where a tool can be downloaded. If a particular concept interests you, you are encouraged to follow up with that article or URL. What you will learn in this study guide is exactly what you need to know to prepare for the CASP+ certification exam. What you will learn from those tips, notes, and URLs is additional context in which the topic at hand may be better understood. Next, we discuss what you should already have in order to be successful when learning from this book.

Requirements: Practice and Experience

To be most successful in reading and learning from this book, you will need to bring something to the table yourself, that is, your experience.

Experience

You're preparing to take one of CompTIA's most advanced certification exams. CompTIA's website associates the CASP+ exam with the SANS Institute GIAC Certified Enterprise Defender (GCED) exam, as only these two exams focus on “cybersecurity practitioner skills” at an advanced level. In comparison, the Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) exams focus on cybersecurity management skills.

The CASP+ exam covers a very wide range of information security topics. Understandably, the range is as wide as the range of information security job disciplines. As each of us grows from a junior level to the higher-level, technical lead roles, the time we spend working in one specialty area overshadows our exposure to other specialties. For example, three senior security practitioners working as an Active Directory engineer, a malware reverse engineer, and a network administrator might be highly skilled in their respective jobs yet have only a simple understanding of each other's roles. The exam topics include specific techniques and technologies that would be familiar to people who have held lead roles in the corresponding area of information security. Someone with experience in one or more technical areas has a great advantage, and that experience will benefit the candidate studying from this book and taking the CASP+ exam.

Last, CompTIA's recommended level of experience is a minimum of 10 years of general hands-on IT experience, including at least five years of hands-on technical security experience. If you have the five years, it is very likely that you have had at least minimal exposure to or understanding of most topics covered, enough for you to benefit from reading this book.

Practice

Given that the certification's title includes the word *practitioner*, you are expected to have, or be capable of building, a home lab for yourself. This does not mean that you need a 42U rack full of servers and network hardware in the basement (though it might bring up a lot of excitement at home). A home lab can be as simple as having one or two virtualized machines (VMs) running on your laptop or desktop with adequate CPU and RAM. This can be done using VirtualBox or VMware Workstation Player, both of which are free. There are many prebuilt VMs available online, designed specifically for security practice. A home lab can be started at little to no cost and be running within 15 minutes. No excuses.

Dedicating some routine time on a home lab will advance your skills and experience as well as demonstrate your passion for the subject. Current and future managers will love it! Seriously, though, when you make time to build, tweak, break, and rebuild systems in your home lab, not only do you readily advance your skills and learn new technologies, but you do so without the consequences of bringing down production.

The final reason for building up a home lab is that it gives you an immediate environment on which to try some of the tools and techniques mentioned in this CASP+ study guide. As with the experience mentioned earlier, your success on the exam is affected by how much you have learned from reading versus how much you understand from doing. The best of success to you on the exam and in your career.

> NOTE Like all exams, the CASP+ certification from CompTIA is updated periodically and may eventually be retired or replaced. At some point after CompTIA is no longer offering this exam, the old editions of our books and online tools will be retired. If you have purchased this book after the exam was retired, or are attempting to register in the Sybex online learning environment after the exam was retired, please know that we make no guarantees that this exam's online Sybex tools will be available once the exam is no longer available.

How to Use This Book

Here is how the book is structured, chapter by chapter:

Chapter 1, "Risk Management" This chapter covers risk management, in particular the security risks surrounding business and industry. The chapter also discusses risk mitigation strategies and controls, including making risk determinations based on a variety of metrics, strategy recommendations based on risk appetite, and business continuity planning.

Chapter 2, "Configure and Implement Endpoint Security Controls" This chapter starts with security controls for host devices. Topics include host hardening, external I/O restrictions, secure operating systems, and several variants of endpoint security software. To wrap up the wide umbrella of network security concepts and architectures, this chapter covers network access control, security zones, and network-enabled devices. Finally, the secure configuration and baselining of network devices are discussed.

Chapter 3, “Security Operations Scenarios” This chapter concentrates on managing threats that require resources such as time, money, and intelligence. This chapter also includes threat management including active hunting for a breach as well as how to proactively protect an organization from compromise.

Chapter 4, “Security Ops: Vulnerability Assessments and Operational Risk” This chapter covers security controls around software vulnerabilities, specific application issues, and operating system vulnerabilities. The chapter also covers material related to incident response and incident recovery. Finally, a large section of the chapter is dedicated to policies and procedures related to security, privacy, and contracts.

Chapter 5, “Compliance and Vendor Risk” This chapter focuses on managing and mitigating vendor risk as well as compliance frameworks and legal considerations and their organizational impact. Emphasis is on integrating diverse industries, many different data considerations, and geographic and legal considerations. It also covers the different regulations, accreditations, and standards that affect cybersecurity.

Chapter 6, “Cryptography and PKI” This chapter covers cryptographic techniques, implementations of both hardware and protocols, and various cryptographic applications.

Chapter 7, “Incident Response and Forensics” This chapter covers research: best practices, research methods, threat intelligence, and the global security community. Additionally, there is related coverage of incident recovery and how severity is determined. This chapter also discusses the research requirements related to contracts. Last, post-incident response, lessons learned, and reporting are also covered.

Chapter 8, “Security Architecture” This chapter covers material related to how business and technology meet in the enterprise environment. In particular, the chapter addresses technical integration of hosts, storage, networks, and applications in an enterprise architecture. Also, this chapter includes coverage of the interaction between business units and their security goals.

Chapter 9, “Secure Cloud and Virtualization” This chapter concentrates on cloud and virtualization technologies. It includes cloud service models, cloud security services, the security-related pros and cons of virtualization, and data security considerations. There is also heavy coverage of several physical and virtual network devices as they relate to security.

Chapter 10, “Mobility and Emerging Technologies” This chapter focuses on mobility and integration with enterprise security, including analysis and impact, implementing security controls, and determining the correct solution for an environment. Coverage of cost-benefit analysis and evaluation of a proposed solution as to its performance, latency, scalability, capability, usability, and maintainability