

Fourth Edition

Save 10%
on Exam Vouchers
Coupon Inside!

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

Take the Next Step
in Your IT Career

Save
10%
on Exam Vouchers*

(up to a \$35 value)

*Some restrictions apply. See web page for details.

CompTIA®

Get details at
www.wiley.com/go/sybextestprep

To get the discount code, you'll need to register and log on the test bank. Then go to Resources.



CompTIA®

CASP+®

Study Guide

Exam CAS-004

Fourth Edition



CompTIA®

CASP+®

Study Guide

Exam CAS-004

Fourth Edition



Nadean H. Tanner

Jeff T. Parker

 **SYBEX®**
A Wiley Brand

Copyright © 2023 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: 978-1-119-80316-4

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

ISBN: 978-1-119-80317-1 (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 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, Sybex, 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. CompTIA and CASP+ are trademarks or registered trademarks of CompTIA, 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 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 electrical 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.

Contents at a Glance

<i>Introduction</i>		<i>xxv</i>
<i>Assessment Test</i>		<i>xxxv</i>
Chapter 1	Risk Management	1
Chapter 2	Configure and Implement Endpoint Security Controls	43
Chapter 3	Security Operations Scenarios	63
Chapter 4	Security Ops: Vulnerability Assessments and Operational Risk	91
Chapter 5	Compliance and Vendor Risk	165
Chapter 6	Cryptography and PKI	211
Chapter 7	Incident Response and Forensics	265
Chapter 8	Security Architecture	301
Chapter 9	Secure Cloud and Virtualization	415
Chapter 10	Mobility and Emerging Technologies	467
Appendix	Answers to Review Questions	505
<i>Index</i>		<i>529</i>

Contents

<i>Introduction</i>		<i>xxv</i>
<i>Assessment Test</i>		<i>xxxv</i>
Chapter 1	Risk Management	1
	Risk Terminology	4
	The Risk Assessment Process	6
	Asset Identification	6
	Information Classification	8
	Risk Assessment	9
	Risk Assessment Options	14
	Implementing Controls	16
	Policies Used to Manage Employees	17
	Pre-Employment Policies	18
	Employment Policies	18
	End of Employment and Termination Procedures	20
	Cost-Benefit Analysis	21
	Continuous Monitoring	22
	Enterprise Security Architecture Frameworks and Governance	23
	Training and Awareness for Users	24
	Best Practices for Risk Assessments	25
	Business Continuity Planning and Disaster Recovery	27
	Reviewing the Effectiveness of Existing Security Controls	28
	Conducting Lessons Learned and After-Action Reviews	30
	Creation, Collection, and Analysis of Metrics	31
	Metrics	31
	Trend Data	32
	Analyzing Security Solutions to Ensure They Meet Business Needs	32
	Testing Plans	33
	Internal and External Audits	34
	Using Judgment to Solve Difficult Problems	35
	Summary	35
	Exam Essentials	36
	Review Questions	38
Chapter 2	Configure and Implement Endpoint Security Controls	43
	Hardening Techniques	45
	Address Space Layout Randomization Use	47
	Hardware Security Module and Trusted Platform Module	48
	Trusted Operating Systems	52
	Compensating Controls	55

	Summary	57
	Exam Essentials	58
	Review Questions	59
Chapter 3	Security Operations Scenarios	63
	Threat Management	66
	Types of Intelligence	66
	Threat Hunting	67
	Threat Emulation	67
	Actor Types	67
	Intelligence Collection Methods	71
	Open-Source Intelligence	71
	Human Intelligence and Social Engineering	73
	Frameworks	74
	MITRE Adversarial Tactics, Techniques and Common Knowledge	74
	ATT&CK for Industrial Control Systems	75
	Cyber Kill Chain	76
	Diamond Model of Intrusion Analysis	76
	Indicators of Compromise	77
	Reading the Logs	77
	Intrusion Detection and Prevention	78
	Notifications and Responses to IoCs	79
	Response	80
	Summary	85
	Exam Essentials	85
	Review Questions	86
Chapter 4	Security Ops: Vulnerability Assessments and Operational Risk	91
	Terminology	97
	Vulnerability Management	98
	Security Content Automation Protocol	103
	Self-Assessment vs. Third-Party Vendor Assessment	105
	Patch Management	108
	Information Sources	110
	Tools	112
	Assessments	124
	Penetration Testing	129
	Assessment Types	131
	Vulnerabilities	134
	Buffer Overflow	134
	Integer Overflow	135
	Memory Leaks	136

	Race Conditions (TOC/TOU)	136
	Resource Exhaustion	137
	Data Remnants	138
	Use of Third-Party Libraries	138
	Code Reuse	138
	Cryptographic Vulnerabilities	138
	Broken Authentication	139
	Security Misconfiguration	140
	Inherently Vulnerable System/Application	140
	Client-Side Processing vs. Server-Side Processing	141
	Attacks	145
	Proactive Detection	153
	Incident Response	153
	Countermeasures	153
	Deceptive Technology	154
	USB Key Drops	155
	Simulation	155
	Security Data Analytics	155
	Application Control	156
	Allow and Block Lists	157
	Security Automation	157
	Physical Security	158
	Summary	159
	Exam Essentials	160
	Review Questions	161
Chapter 5	Compliance and Vendor Risk	165
	Shared Responsibility in Cloud Computing	168
	Cloud Service/Infrastructure Models	169
	Cloud Computing Providers and Hosting Options	169
	Benefits of Cloud Computing	171
	Security of On-Demand/Elastic Cloud Computing	174
	Geographic Location	175
	Infrastructure	175
	Compute	175
	Storage	175
	Networking	176
	Managing and Mitigating Risk	182
	Security Concerns of Integrating Diverse Industries	185
	Regulations, Accreditations, and Standards	187
	PCI DSS	187
	GDPR	190
	ISO	192
	CMMI	193

	NIST	194
	COPPA	195
	CSA-STAR	196
	HIPAA, SOX, and GLBA	197
	Contract and Agreement Types	198
	Third-Party Attestation of Compliance	202
	Legal Considerations	203
	Summary	204
	Exam Essentials	205
	Review Questions	206
Chapter 6	Cryptography and PKI	211
	The History of Cryptography	216
	Cryptographic Goals and Requirements	217
	Supporting Security Requirements	218
	Compliance and Policy Requirements	219
	Privacy and Confidentiality Requirements	219
	Integrity Requirements	220
	Nonrepudiation	220
	Risks with Data	221
	Data at Rest	221
	Data in Transit	222
	Data in Process/Data in Use	222
	Hashing	223
	Message Digest	225
	Secure Hash Algorithm	225
	Message Authentication Code	226
	Hashed Message Authentication Code	226
	RACE Integrity Primitives Evaluation Message Digest	226
	Poly1305	226
	Symmetric Algorithms	227
	Data Encryption Standard	230
	Triple DES	231
	Rijndael and the Advanced Encryption Standard	231
	ChaCha	232
	Salsa20	232
	International Data Encryption Algorithm	232
	Rivest Cipher Algorithms	233
	Counter Mode	233
	Asymmetric Encryption	233
	Diffie–Hellman	235
	RSA	236
	Elliptic Curve Cryptography	237

ElGamal	238
Hybrid Encryption and Electronic Data Exchange (EDI)	238
Public Key Infrastructure Hierarchy	239
Certificate Authority	240
Registration Authority	241
Digital Certificates	241
Certificate Revocation List	243
Certificate Types	243
Certificate Distribution	244
The Client’s Role in PKI	245
Implementation of Cryptographic Solutions	247
Application Layer Encryption	248
Transport Layer Encryption	249
Internet Layer Controls	250
Additional Authentication Protocols	251
Cryptocurrency	252
Digital Signatures	252
Recognizing Cryptographic Attacks	254
Troubleshooting Cryptographic Implementations	256
Summary	259
Exam Essentials	259
Review Questions	261

Chapter 7 Incident Response and Forensics 265

The Incident Response Framework	268
Event Classifications	268
Triage Events	269
Pre-Escalation Tasks	270
The Incident Response Process	270
Response Playbooks and Processes	273
Communication Plan and Stakeholder Management	274
Forensic Concepts	277
Principles, Standards, and Practices	278
The Forensic Process	279
Forensic Analysis Tools	283
File Carving Tools	284
Binary Analysis Tools	284
Analysis Tools	286
Imaging Tools	288
Hashing Utilities	289
Live Collection vs. Postmortem Tools	290
Summary	294
Exam Essentials	294
Review Questions	295

Chapter 8	Security Architecture	301
	Security Requirements and Objectives for a Secure Network	
	Architecture	310
	Services	310
	Segmentation	334
	Deperimeterization/Zero Trust	344
	Merging Networks from Various Organizations	352
	Software-Defined Networking	357
	Organizational Requirements for Infrastructure Security Design	358
	Scalability	358
	Resiliency	359
	Automation	359
	Containerization	360
	Virtualization	361
	Content Delivery Network	361
	Integrating Applications Securely into an Enterprise Architecture	362
	Baseline and Templates	362
	Software Assurance	367
	Considerations of Integrating Enterprise Applications	370
	Integrating Security into the Development Life Cycle	373
	Data Security Techniques for Securing Enterprise Architecture	384
	Data Loss Prevention	384
	Data Loss Detection	387
	Data Classification, Labeling, and Tagging	388
	Obfuscation	390
	Anonymization	390
	Encrypted vs. Unencrypted	390
	Data Life Cycle	391
	Data Inventory and Mapping	391
	Data Integrity Management	391
	Data Storage, Backup, and Recovery	392
	Security Requirements and Objectives for Authentication	
	and Authorization Controls	394
	Credential Management	394
	Password Policies	396
	Federation	398
	Access Control	399
	Protocols	401
	Multifactor Authentication	403
	One-Time Passwords	404
	Hardware Root of Trust	404
	Single Sign-On	405

	JavaScript Object Notation Web Token	405
	Attestation and Identity Proofing	406
	Summary	406
	Exam Essentials	407
	Review Questions	410
Chapter 9	Secure Cloud and Virtualization	415
	Implement Secure Cloud and Virtualization Solutions	418
	Virtualization Strategies	419
	Deployment Models and Considerations	425
	Service Models	429
	Cloud Provider Limitations	433
	Extending Appropriate On-Premises Controls	433
	Storage Models	439
	How Cloud Technology Adoption Impacts Organization Security	445
	Automation and Orchestration	445
	Encryption Configuration	445
	Logs	446
	Monitoring Configurations	447
	Key Ownership and Location	448
	Key Life-Cycle Management	448
	Backup and Recovery Methods	449
	Infrastructure vs. Serverless Computing	450
	Software-Defined Networking	450
	Misconfigurations	451
	Collaboration Tools	451
	Bit Splitting	461
	Data Dispersion	461
	Summary	461
	Exam Essentials	462
	Review Questions	463
Chapter 10	Mobility and Emerging Technologies	467
	Emerging Technologies and Their Impact on Enterprise	
	Security and Privacy	471
	Artificial Intelligence	472
	Machine Learning	472
	Deep Learning	472
	Quantum Computing	473
	Blockchain	473
	Homomorphic Encryption	474
	Distributed Consensus	475
	Big Data	475

	Virtual/Augmented Reality	475
	3D Printing	476
	Passwordless Authentication	476
	Nano Technology	477
	Biometric Impersonation	477
	Secure Enterprise Mobility Configurations	478
	Managed Configurations	479
	Deployment Scenarios	486
	Mobile Device Security Considerations	487
	Security Considerations for Technologies, Protocols, and Sectors	495
	Embedded Technologies	495
	ICS/Supervisory Control and Data Acquisition	496
	Protocols	498
	Sectors	499
	Summary	500
	Exam Essentials	500
	Review Questions	501
Appendix	Answers to Review Questions	505
	Chapter 1: Risk Management	506
	Chapter 2: Configure and Implement Endpoint	
	Security Controls	507
	Chapter 3: Security Operations Scenarios	509
	Chapter 4: Security Ops: Vulnerability Assessments	
	and Operational Risk	511
	Chapter 5: Compliance and Vendor Risk	513
	Chapter 6: Cryptography and PKI	514
	Chapter 7: Incident Response and Forensics	516
	Chapter 8: Security Architecture	519
	Chapter 9: Secure Cloud and Virtualization	522
	Chapter 10: Mobility and Emerging Technologies	524
	<i>Index</i>	529

Table of Exercises

Exercise	1.1	Calculating Annualized Loss Expectancy	12
Exercise	1.2	Reviewing the Employee Termination Process	21
Exercise	2.1	Running a Security Scanner to Identify Vulnerabilities	50
Exercise	2.2	Bypassing Command Shell Restrictions	51
Exercise	3.1	Using WinDump to Sniff Traffic	79
Exercise	3.2	Reviewing and Assessing ACLs	84
Exercise	4.1	Tracking Vulnerabilities in Software	103
Exercise	4.2	Performing Passive Reconnaissance on Your Company, School, or Another Organization	114
Exercise	5.1	What Services Should Be Moved to the Cloud?	171
Exercise	5.2	Identifying Risks and Issues with Cloud Computing	180
Exercise	5.3	Reviewing Documents	200
Exercise	8.1	Configuring iptables	317
Exercise	8.2	Using Pingdom Full Page Test	323
Exercise	8.3	Testing Your Antivirus Program	333
Exercise	8.4	Reviewing and Assessing ACLs	343
Exercise	9.1	Creating a Virtual Machine	420
Exercise	9.2	Identifying What Services Should Be Moved to the Cloud	428
Exercise	9.3	Identifying Risks and Issues with Cloud Computing	436
Exercise	9.4	Understanding Online Storage	441
Exercise	9.5	Turning to the Cloud for Storage and Large File Transfer	444
Exercise	9.6	Eavesdropping on Web Conferences	452
Exercise	9.7	Sniffing Email with Wireshark	457
Exercise	9.8	Sniffing VoIP with Cain & Abel	459

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.



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.



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.



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.