

6th Edition



SSCP®

Systems Security
Certified Practitioner

An (ISC)² Certification

The Official (ISC)²
SSCP® CBK® Reference

Michael S. Wills, SSCP, CISSP, CAMS

 **SYBEX**
A Wiley Brand

Table of Contents

[Cover](#)

[Title Page](#)

[Copyright](#)

[Acknowledgments](#)

[About the Author](#)

[About the Technical Editor](#)

[Foreword](#)

[Introduction](#)

[ABOUT THIS BOOK](#)

[WHERE DO YOU GO FROM HERE?](#)

[LET'S GET STARTED!](#)

[HOW TO CONTACT THE PUBLISHER](#)

[NOTES](#)

[CHAPTER 1: Security Operations and Administration](#)

[COMPLY WITH CODES OF ETHICS](#)

[UNDERSTAND SECURITY CONCEPTS](#)

[DOCUMENT, IMPLEMENT, AND MAINTAIN
FUNCTIONAL SECURITY CONTROLS](#)

[PARTICIPATE IN ASSET MANAGEMENT](#)

[IMPLEMENT SECURITY CONTROLS AND ASSESS
COMPLIANCE](#)

[PARTICIPATE IN CHANGE MANAGEMENT](#)

[PARTICIPATE IN SECURITY AWARENESS AND
TRAINING](#)

[PARTICIPATE IN PHYSICAL SECURITY
OPERATIONS](#)

SUMMARY

CHAPTER 2: Access Controls

ACCESS CONTROL CONCEPTS

IMPLEMENT AND MAINTAIN AUTHENTICATION METHODS

SUPPORT INTERNETWORK TRUST ARCHITECTURES

PARTICIPATE IN THE IDENTITY MANAGEMENT LIFECYCLE

IMPLEMENT ACCESS CONTROLS

SUMMARY

CHAPTER 3: Risk Identification, Monitoring, and Analysis

DEFEATING THE KILL CHAIN ONE SKIRMISH AT A TIME

UNDERSTAND THE RISK MANAGEMENT PROCESS

PERFORM SECURITY ASSESSMENT ACTIVITIES

OPERATE AND MAINTAIN MONITORING SYSTEMS

ANALYZE MONITORING RESULTS

SUMMARY

NOTES

CHAPTER 4: Incident Response and Recovery

SUPPORT THE INCIDENT LIFECYCLE

UNDERSTAND AND SUPPORT FORENSIC INVESTIGATIONS

UNDERSTAND AND SUPPORT BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY PLAN ACTIVITIES

CIANA+PS AT LAYER 8 AND ABOVE

SUMMARY

CHAPTER 5: Cryptography

UNDERSTAND FUNDAMENTAL CONCEPTS OF CRYPTOGRAPHY

CRYPTOGRAPHIC ATTACKS, CRYPTANALYSIS, AND COUNTERMEASURES

UNDERSTAND THE REASONS AND REQUIREMENTS FOR CRYPTOGRAPHY

UNDERSTAND AND SUPPORT SECURE PROTOCOLS

UNDERSTAND PUBLIC KEY INFRASTRUCTURE SYSTEMS

SUMMARY

NOTES

CHAPTER 6: Network and Communications Security

UNDERSTAND AND APPLY FUNDAMENTAL CONCEPTS OF NETWORKING

IPV4 ADDRESSES, DHCP, AND SUBNETS

IPV4 VS. IPV6: KEY DIFFERENCES AND OPTIONS

UNDERSTAND NETWORK ATTACKS AND COUNTERMEASURES

MANAGE NETWORK ACCESS CONTROLS

MANAGE NETWORK SECURITY

OPERATE AND CONFIGURE NETWORK-BASED SECURITY DEVICES

OPERATE AND CONFIGURE WIRELESS TECHNOLOGIES

SUMMARY

NOTES

CHAPTER 7: Systems and Application Security

SYSTEMS AND SOFTWARE INSECURITY

INFORMATION SECURITY = INFORMATION
QUALITY + INFORMATION INTEGRITY

IDENTIFY AND ANALYZE MALICIOUS CODE AND
ACTIVITY

IMPLEMENT AND OPERATE ENDPOINT DEVICE
SECURITY

OPERATE AND CONFIGURE CLOUD SECURITY

OPERATE AND SECURE VIRTUAL
ENVIRONMENTS

SUMMARY

NOTES

Appendix: Cross-Domain Challenges

PARADIGM SHIFTS IN INFORMATION SECURITY?

PIVOT 1: TURN THE ATTACKERS' PLAYBOOKS
AGAINST THEM

PIVOT 2: CYBERSECURITY HYGIENE: THINK
SMALL, ACT SMALL

PIVOT 3: FLIP THE "DATA-DRIVEN VALUE
FUNCTION"

PIVOT 4: OPERATIONALIZE SECURITY ACROSS
THE IMMEDIATE AND LONGER TERM

PIVOT 5: ZERO-TRUST ARCHITECTURES AND
OPERATIONS

OTHER DANGERS ON THE WEB AND NET
CURIOSITY AS COUNTERMEASURE

NOTES

Index

End User License Agreement

List of Tables

Introduction

[TABLE I.1 Kill Chain Phases Mapped to Chapters](#)

Chapter 1

[TABLE 1.1 Forms of Intellectual Property Protection](#)

Chapter 4

[TABLE 4.1 Indicators, Alarms, and IOCs](#)

[TABLE 4.2 Security Events and Response Priorities](#)

Chapter 5

[TABLE 5.1 Overview of Block Ciphers](#)

[TABLE 5.2 Common Stream Ciphers](#)

Chapter 6

[TABLE 6.1 OSI and TCP/IP Datagram Naming](#)

[TABLE 6.2 IPv4 Address Classes](#)

[TABLE 6.3 Address Classes and CIDR](#)

[TABLE 6.4 Important Characteristics for Common Network Cabling Types](#)

[TABLE 6.5 Commonly Used Security and Access Control Protocols and Port Numbe...](#)

[TABLE 6.6 Commonly Used Network Management Protocols and Port Numbers](#)

[TABLE 6.7 Commonly Used Email Protocols and Port Numbers](#)

[TABLE 6.8 Commonly Used Web Page Access Protocols and Port Numbers](#)

[TABLE 6.9 Commonly Used Utility Protocols and Port Numbers](#)

[TABLE 6.10 Wireless Connections Overview](#)

[TABLE 6.11 IEEE 802.11 Standard Amendments](#)

[TABLE 6.12 Basic Overview of Cellular Wireless Technologies](#)

List of Illustrations

Introduction

[FIGURE I.1 MITRE's ATT&CK cybersecurity kill chain model](#)

Chapter 1

[FIGURE 1.1 The DIKW knowledge pyramid](#)

[FIGURE 1.2 ISO 27002 phases](#)

[FIGURE 1.3 AWS dashboard](#)

Chapter 2

[FIGURE 2.1 Subjects and objects](#)

[FIGURE 2.2 US-CERT Traffic Light Protocol for information classification and...](#)

[FIGURE 2.3 Bell-LaPadula \(a\) versus Biba access control models \(b\).](#)

[FIGURE 2.4 Crossover error rate](#)

Chapter 3

[FIGURE 3.1 Kill chain conceptual model](#)

[FIGURE 3.2 Target 2013 data breach kill chain](#)

[FIGURE 3.3 Four bases of risk, viewed together](#)

[FIGURE 3.4 Risk timeline](#)

[FIGURE 3.5 ISO 31000 RMF](#)

[FIGURE 3.6 PCI-DSS goals and requirements](#)

Chapter 4

[FIGURE 4.1 Triage: from precursors to incident response](#)

[FIGURE 4.2 Incident response lifecycle](#)

[FIGURE 4.3 NIST incident handling checklist](#)

[FIGURE 4.4 Indicators of a kill chain in action](#)

[FIGURE 4.5 The descent from anomaly to organizational death](#)

[FIGURE 4.6 Continuity of operations planning and supporting planning process...](#)

[FIGURE 4.7 Beyond the seventh layer](#)

Chapter 5

[FIGURE 5.1 Crypto family tree](#)

[FIGURE 5.2 Comparing hashing and encryption as functions](#)

[FIGURE 5.3 Notional S-box](#)

[FIGURE 5.4 Notional P-box](#)

[FIGURE 5.5 Feistel encryption and decryption \(notional\)](#)

[FIGURE 5.6 CBC mode](#)

[FIGURE 5.7 CFB mode](#)

[FIGURE 5.8 CTR mode](#)

[FIGURE 5.9 ECB with small block size weaknesses showing](#)

[FIGURE 5.10 RC4 stream cipher](#)

[FIGURE 5.11 Diffie-Hellman-Merkle shared key generation \(conceptual\)](#)

[FIGURE 5.12 TLS handshake](#)

[FIGURE 5.13 The blockchain concept](#)

[FIGURE 5.14 Chains of trust](#)

[FIGURE 5.15 Certification path validation algorithm](#)

Chapter 6

[FIGURE 6.1 Wrapping: layer-by-layer encapsulation](#)

[FIGURE 6.2 DNS resolver in action](#)

[FIGURE 6.3 DNS caching](#)

[FIGURE 6.4 Dynamic routing protocols family tree](#)

[FIGURE 6.5 OSI Seven-Layer Reference Model](#)

[FIGURE 6.6 IPv4 packet format](#)

[FIGURE 6.7 TCP three-way handshake](#)

[FIGURE 6.8 OSI and TCP/IP side-by-side comparison](#)

[FIGURE 6.9 TCP flag fields](#)

[FIGURE 6.10 Changes to packet header from IPv4 to IPv6](#)

[FIGURE 6.11 A ring topography](#)

[FIGURE 6.12 A star topography](#)

[FIGURE 6.13 A mesh topography](#)

[FIGURE 6.14 Man-in-the-middle attack](#)

[FIGURE 6.15 Smurfing attack](#)

[FIGURE 6.16 Network access control in context](#)

[FIGURE 6.17 Remote access in context](#)

[FIGURE 6.18 Common areas of increased risk in remote access](#)

[FIGURE 6.19 Extranet advantages and disadvantages](#)

[FIGURE 6.20 Perimeter net and screened hosts](#)

Chapter 7

[FIGURE 7.1 Cloud service models](#)

Appendix

[FIGURE A.1 Zero-trust architecture logical core](#)

The Official (ISC)2® SSCP® CBK® Reference

Sixth Edition

MICHAEL S. WILLS, SSCP, CISSP, CAMS



Copyright © 2022 by (ISC)²

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

Published simultaneously in Canada.

978-1-119-87486-7

978-1-119-87488-1 (ebk.)

978-1-119-87487-4 (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 <http://www.wiley.com/go/permission>.

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Website is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Website may provide or recommendations it may make. Further, readers should be aware the Internet Websites listed in this work may have changed or disappeared between when this work was written and when it is read.

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: 2022930202

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. (ISC)², SSCP, and CBK are registered trademarks or certification marks of International Information Systems 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.

Cover design: Wiley and (ISC)²

Acknowledgments

This newly revised sixth edition that you hold in your hands is the culmination of more than a year of effort with the team at (ISC)² that I had the privilege of working with. This Common Book of Knowledge reflects the consensus across that team of the know-how that SSCPs need, on the job, to be part of maintaining the safety, security, integrity, and availability of the information systems we all depend upon.

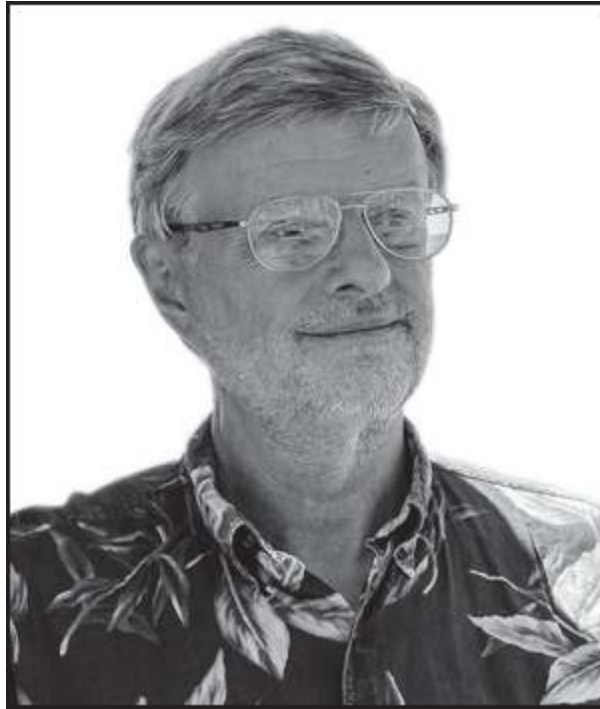
Where it achieves that objective, and provides you value in the years to come—is a testament to the generosity of everyone on that combined set of project teams in sharing their insights with me. (And where it fails to work well, or work at all, it's my own darned fault.) Countless hours on Zoom and Webex with subject-matter experts like Graham Thornburrow-Dobson, John Warsinski, Maytal Brooks-Kempler, Laural Hargadon, and Fabio Cerullo sharpened my thinking and focused my writing more toward the operational aspects of cybersecurity and less on the theoretical. A special thank-you too goes out to Kaitlyn Langenbacher, the project owner for those updates at (ISC)², and all of the editors and proofreaders working with her; throughout all of that, the support, questions, and co-creativity they brought made this work a truly joint, collaborative one. I would also like to acknowledge my faculty teammates here at Embry-Riddle Aeronautical University for sharing their frank and candid views throughout many conversations on making this body of knowledge accessible and engaging in the classroom. The ideas and experiences of Drs. Aaron Glassman and Jason Clark have also profoundly affected my approach to what you see before you here in this book.

Since this book needed to speak to troubleshooters, I drew on decades of teaching I'd received from many professionals in the military, in government, and in the private sector about the fine art and brute-force cybernetics of debugging networks, systems, highly secure communications systems, and all of the arcana of controlling space-based systems working many different missions. I've also drawn on years of working with small and medium but otherwise rather down-to-earth business IT systems and what it took to get them back into operations. Where that problem-solving focus comes through clearly and helps you shoot the troubles you have to deal with, I owe a great debt of thanks to those who let me learn how in real time.

Without the tireless support of the editorial team at Wiley/Sybex—especially Jim Minatel and Pete Gaughan—I think I'd still be struggling with unflowing the lessons and reflowing them into reference and troubleshooting memory-joggers. The technical review by Graham Thornburrow-Dobson, as well as by Tara Zeiler and Fabio Cerullo at (ISC)², have all helped make what you have in your hands right now deliver the right content in the best way possible. Tracy Brown, Barath Kumar Rajasekaran, Kim Wimpsett, and the rest of the team of proofreaders and copyeditors made it all look great too! Any remaining mistakes, omissions, or confusing passages that remain are mine and no one else's; let me know please when you find one!

Finally, I wish to thank my wife Nancy. She saved my life and brought me peace. Her strength inspired me to say “yes” one more time when Jim called me, again, about doing this book, and she has kept both of us healthy and happy throughout. We go together, on adventures like writing, and on ones for which we do need to pack a pocket handkerchief.

About the Author



Michael S. Wills, SSCP, CISSP, CAMS, is Assistant Professor of Applied and Innovative Information Technologies at the College of Business, Embry-Riddle Aeronautical University—Worldwide, where he continues his graduate and undergraduate teaching and research in cybersecurity and information assurance.

Mike has also been an advisor on science and technology policy to the UK's Joint Intelligence Committee, Ministry of Justice, and Defense Science and Technology Laboratories, helping them to evolve an operational and policy consensus relating topics from cryptography and virtual worlds, through the burgeoning surveillance society, to the proliferation of weapons of mass disruption (not just “destruction”) and their effects on global, regional, national, and personal security. For a time, this had him

sometimes known as the UK's nonresident expert on outer space law.

Mike has been supporting the work of (ISC)² by writing, editing, and updating books, study guides, and course materials for both their SSCP and CISSP programs. He wrote the *SSCP Official Study Guide 2nd Edition* in 2019, followed quickly by the *SSCP Official Common Book of Knowledge 5th Edition*. He was lead author for the 2021 update of (ISC)²'s official CISSP and SSCP training materials. Mike has also contributed to several industry roundtables and white papers on digital identity and cyber fraud detection and prevention and has been a panelist and webinar presenter on these and related topics for ACAMS.

Mike earned his BS and MS degrees in computer science, both with minors in electrical engineering, from Illinois Institute of Technology, and his MA in Defence Studies from King's College, London. He is a graduate of the Federal Chief Information Officer program at National Defense University and the Program Manager's Course at Defense Systems Management College.

Mike and his wife Nancy currently call Wexford, Ireland, their home. Living abroad since the end of the last century, they find new perspectives, shared values, and wonderful people wherever they go. As true digital nomads, it's getting time to move again. Where to? They'll find out when they get there.

About the Technical Editor

Graham Thornburrow-Dobson, CISSP, SSCP, is a security consultant and instructor with more than 30 years of experience in IT, with 20 years focused on IT security and related training.

Graham is an authorized (ISC)² instructor who has delivered security training to a wide range of security professionals globally via both classroom-based and online training.

Graham has also been supporting the efforts of (ISC)² in the continued development of their CISSP, SSCP, and ISSAP programs as both a writer and a technical editor.

Graham currently resides in Lincolnshire, United Kingdom. Graham would add more, but, hey, security!

Foreword



WELCOME TO *THE OFFICIAL* (ISC)² SSCP CBK

Reference! By picking up this book, you have demonstrated your commitment to continuing your professional education and have made the decision to take the next step in your career.

An (ISC)² Systems Security Certified Practitioner (SSCP) credential shows an understanding of and proficiency with the hands-on technical work that is needed in the information security field. The certification is ideal for IT professionals responsible for the hands-on operational security of their organizations' critical assets, including those in positions such as network security engineers, systems administrators and engineers, security analysts, consultants and administrators, database administrators, and network analysts.

It demonstrates that you closely follow best practices, policies, and procedures in accordance with the SSCP Common Body of Knowledge. Whether you are using this guide to supplement your preparation to sit for the exam or you are an existing SSCP member using this as a reference, this book helps to facilitate the practical knowledge you need to assure strong information security for your organization's daily operations.

(ISC)² promotes the development of information security professionals throughout the world. As an SSCP with all the benefits of (ISC)² membership, you will become part of a global network of more than 160,000 certified professionals who are working to inspire a safe and secure cyber world. By becoming a member of (ISC)² you will have also officially committed to ethical conduct that aligns with your position of trust as a cybersecurity professional.

Reflecting the most pertinent issues that security practitioners currently face, along with the best practices for mitigating those issues, *The Official (ISC)² SSCP CBK Reference* offers step-by-step guidance through the seven different domains included in the exam, which are:

- Access Controls
- Security Operations and Administration
- Risk Identification, Monitoring and Analysis
- Incident Response and Recovery
- Cryptography
- Networks and Communications Security
- Systems and Application Security

Drawing from a comprehensive, up-to-date global body of knowledge, this book prepares you to join thousands of

practitioners worldwide who have obtained the SSCP. For those with proven technical skills and practical security knowledge, the SSCP certification is the ideal credential. The SSCP confirms the breadth and depth of practical security knowledge expected of those in hands-on operational IT roles. The certification provides industry-leading confirmation of a practitioner's ability to implement, monitor, and administer information security policies and procedures that ensure data confidentiality, integrity, and availability (CIA).

The goal for SSCP credential holders is to achieve the highest standard for cybersecurity expertise—managing multiplatform IT systems while keeping sensitive data secure. This becomes especially crucial in the era of digital transformation, where cybersecurity permeates virtually every data stream. Organizations that can demonstrate world-class cybersecurity capabilities and trusted transaction methods enable customer loyalty and fuel success.

The opportunity has never been greater for dedicated professionals like yourself to carve out a meaningful career and make a difference in their organizations. *The Official (ISC)² SSCP CBK Reference* will be your constant companion in protecting and securing the critical data assets of your organization, and it will serve you for years to come as you progress in your career.

I wish you luck on the exam and success in your next step along your career path.

Best regards,

A handwritten signature in black ink that reads "Chris Rosso". The signature is written in a cursive, flowing style with a large initial "C" and "R".

Clar Rosso, CEO, (ISC)²

Introduction

CONGRATULATIONS ON CHOOSING TO become a Systems Security Certified Practitioner (SSCP)! In making this choice, you're signing up to join the professionals who strive to keep our information-based modern world safe, secure, and reliable. SSCPs and other information security professionals help businesses and organizations keep private data *private* and help to ensure that published and public-facing information stays unchanged and unhacked.

Whether you are new to the fields of information security, information assurance, or cybersecurity, or you've been working with these concepts, tools, and ideas for some time now, this book is here to help you grow your knowledge, skills, and abilities as a systems security professional.

Let's see how!

ABOUT THIS BOOK

You're here because you need a ready reference source of ideas, information, knowledge, and experience about information systems security. Users of earlier editions of the CBK describe it as the place to go when you need to look up something about bringing your systems or networks back up and online—when you can't exactly Google it. As a first responder in an information security incident, you may need to rely on what you know and what you've got at hand as you characterize, isolate, and contain an intruder and their malware or other causal agents. This book cannot answer all of the questions you'll have in real time, but it may just remind you of important concepts as well as critical details when you need them. As with any reference work, it can help you think your way through to a

solution. By taking key definitions and concepts and *operationalizing* them, showing how they work in practice, this book can enrich the checklists, troubleshooting guides, and task-focused procedures that you may already be using in your work.

The SSCP Seven Domains

This book directly reflects the SSCP Common Body of Knowledge, which is the comprehensive framework that (ISC)² has developed to express what security professionals should have working knowledge of. These domains include theoretical knowledge, industry best practices, and applied skills and techniques. Chapter by chapter, this book takes you through these domains, with major headings within each chapter being your key to finding what you need when you need it. Topics that are covered in more than one domain will be found within sections or subsections in each chapter as appropriate.

This Sixth Edition has been updated to reflect (ISC)²'s Domain Content Outline, released in November 2021. This outline update changed the relative order of the first two domains, but largely kept the topics within each domain the same. Revisions, clarifications, and additions have been made throughout, while a new [Appendix](#) brings topics from across those Domains together to provide you assistance with today's thorniest of information security challenges.

(ISC)² is committed to helping members learn, grow, and thrive. The Common Body of Knowledge (CBK) is the comprehensive framework that helps it fulfill this commitment. The CBK includes all the relevant subjects a security professional should be familiar with, including skills, techniques, and best practices. (ISC)² uses the various domains of the CBK to test a certificate candidate's levels of expertise in the most critical aspects of

information security. You can see this framework in the SSCP Exam Outline at

<https://www.isc2.org/-/media/ISC2/Certifications/Exam-Outlines/2021/SSCP-Exam-Outline-English-Nov-2021.ashx?la=en&hash=ABCB9E34548D2E8170ADA04EAAD3003F5577D3F5>

Successful candidates are competent in the following seven domains:

Domain 1 Security Operations and Administration

Identification of information assets and documentation of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability, such as:

- 1.1 Comply with codes of ethics.
- 1.2 Understand security concepts.
- 1.3 Identify and implement security controls.
- 1.4 Document and maintain functional security controls.
- 1.5 Participate in asset management lifecycle (hardware, software, and data).
- 1.6 Participate in change management lifecycle.
- 1.7 Participate in implementing security awareness and training (e.g., social engineering/phishing).
- 1.8 Collaborate with physical security operations (e.g., data center assessment, badging).

Domain 2 Access Controls Policies, standards, and procedures that define users (human and nonhuman) as entities with identities that are approved to use an organization's systems and information assets, what they can do, which resources and information they can access, and what operations they can perform on a system, such as:

2.1 Implement and maintain authentication methods.

2.2 Support internetwork trust architectures.

2.3 Participate in the identity management lifecycle.

2.4 Understand and apply access controls.

Domain 3 Risk Identification, Monitoring, and Analysis

Risk identification is the review, analysis, and implementation of processes essential to the identification, measurement, and control of loss associated with unplanned adverse events.

Monitoring and analysis are determining system implementation and access in accordance with defined IT criteria. This involves collecting information for identification of, and response to, security breaches or events, such as:

3.1 Understand the risk management process.

3.2 Understand legal and regulatory concerns (e.g., jurisdiction, limitations, privacy).

3.3 Participate in security assessment and vulnerability management activities.

3.4 Operate and monitor security platforms (e.g., continuous monitoring).

3.5 Analyze monitoring results.

Domain 4 Incident Response and Recovery

Prevent. Detect. Respond. Recover. Incident response and recovery focus on the near real-time actions that must take place if the organization is to survive a cyberattack or other information security incident, get back into operation, and continue as a viable entity. In this domain, the SSCP gains an understanding of how

to handle incidents using consistent, applied approaches within a framework of business continuity planning (BCP) and disaster recovery planning (DRP). These approaches are utilized to mitigate damages, recover business operations, and avoid critical business interruption:

- 4.1 Support incident lifecycle (e.g., National Institute of Standards and Technology [NIST], International Organization for Standardization [ISO]).
- 4.2 Understand and support forensic investigations.
- 4.3 Understand and support business continuity plan (BCP) and disaster recovery plan (DRP) activities.

Domain 5 Cryptography The protection of information using techniques that ensure its integrity, confidentiality, authenticity, and nonrepudiation, and the

recovery of encrypted information in its original form:

- 5.1 Understand reasons and requirements for cryptography.
- 5.2 Apply cryptography concepts.
- 5.3 Understand and implement secure protocols.
- 5.4 Understand and support public key infrastructure (PKI) systems.

Domain 6 Network and Communications Security The network structure, transmission methods and techniques, transport formats, and security measures used to operate both private and public communication networks:

6.1 Understand and apply fundamental concepts of networking.

6.2 Understand network attacks (e.g., distributed denial of service [DDoS], man-in-the-middle [MITM], Domain Name System [DNS] poisoning) and countermeasures (e.g., content delivery networks [CDN]).

6.3 Manage network access controls.

6.4 Manage network security.

6.5 Operate and configure network-based security devices.

6.6 Secure wireless communications.

Domain 7 Systems and Application Security

Countermeasures and prevention techniques for dealing with viruses, worms, logic bombs, Trojan horses, and other related forms of intentionally created damaging code:

7.1 Identify and analyze malicious code and activity.

7.2 Implement and operate endpoint device security.

7.3 Administer Mobile Device Management (MDM).

7.4 Understand and configure cloud security.

7.5 Operate and maintain secure virtual environments.

Appendix: Cross-Domain Challenges In 2020 and 2021, the world was rocked by the Covid-19 pandemic and a significant increase in the complexity, scale, and severity of cybercrime and cyber attacks on businesses, government services, and critical infrastructures. In response, information security professionals around the globe worked tirelessly to address incident response

and recovery. They also worked to improve systems hardening and intrusion detection techniques. Many of the persistent (and pernicious) attack strategies exploit aspects of nearly every topic in every SSCP Domain. Here in the CBK, the [appendix](#) offers five sets of strategies that can help security professionals shift the offense-versus-defense struggle more into the defense's favor. These five shifts or *pivots* are:

- Turn the attackers' playbooks against them.
- Cybersecurity hygiene: think small, act small.
- Flip the “data-driven value function.”
- Operationalizing security across the immediate and longer term.
- Zero-trust architectures and operations.

The [appendix](#) also helps put the challenges of maintaining information security at the interface between an organization's IT systems and its *operational technology (OT)* ones. Since 2019, cyber attacks on process controls, autonomous devices, smart buildings elements, and Internet of Things (IoT) systems have disrupted many organizations. The pressure is on for SSCPs and other information security professionals to better understand the security and safety issues related to how their organization's data actually makes physical actions take place; the [appendix](#) provides you some places to start.

Using This Book to Defeat the Cybersecurity Kill Chain

Your employers or clients have entrusted the safety and security of their information systems to you, as one of their on-site information security professionals. Those systems are under constant attack—not just the threat of attack.

Each day, the odds are great that somebody is knocking at your electronic front doors, trying the e-window latches on your organization's web pages, and learning about your information systems and how you use them. That's reconnaissance in action, the first step in the cybersecurity kill chain.

As an SSCP you're no doubt aware of the cybersecurity kill chain, as a summary of how advanced persistent threat (APT) actors plan and conduct their attacks against many private and public organizations, their IT infrastructures, and their information assets and systems. Originally developed during the 1990s by applying military planning doctrines of effects-based targeting, this kill chain is similar to the value chain concept used by businesses and public-sector organizations around the world. Both value chains and kill chains start with the objective—the desired end state or result—and work backward, all the way back to choosing the right targets to attack in the first place.¹ Lockheed-Martin first published its cybersecurity kill chain in 2011; the MITRE Corporation, a federally funded research and development corporation (FFRDC), expanded on this in 2018 with its threat-based Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework. ATT&CK takes the kill chain concept down into the tactics, techniques, and procedures used by squad-level and individual soldiers in the field. (Note that in military parlance, planning flows from strategic, through operational, to tactical; but common business-speak usage flips the names of the last two steps, looking at business operations as being the point-of-contact steps with customers, and the tactical layer of planning translating strategic objectives into manageable, measurable, value-producing packages of work.) ATT&CK as a framework is shown in [Figure I.1](#), highlighting the two major phases that defenders need to be aware of and engaged with: prestrike