(ISC)^2®

FOURTH EDITION

THE OFFICIAL (ISC)^2® GUIDE TO THE SSCP® CBK®

Gordon/Hernandez

- Produced by (ISC)^2, the trusted global source of industry expertise for information security
- The definitive body of knowledge used by candidates for the Systems Security Certified Practitioner (SSCP) credential

SSCP®

Systems Security
Certified Practitioner

SYBEX
A Wiley Brand

The Official (ISC)$^{2®}$ Guide to the SSCP® CBK®

Fourth Edition

ADAM GORDON

CISSP-ISSAP, CISSP-ISSMP, SCCP, CCSP, CISA, CRISC

STEVEN HERNANDEZ

MBA, HCISPP, CISSP, CSSLP, SSCP, CAP, CISA

(ISC)$^{2®}$

SYBEX®
A Wiley Brand

The Official (ISC)$^{2®}$ Guide to the SSCP® CBK®, Fourth Edition

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published by John Wiley & Sons, Inc., Indianapolis, Indiana
Published simultaneously in Canada

ISBN: 978-1-119-27863-4
ISBN: 978-1-119-27864-1 (ebk)
ISBN: 978-1-119-27865-8 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

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 Web site 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 that 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 please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2016937576

About the Editors

Adam Gordon With over 25 years of experience as both an educator and IT professional, Adam holds numerous professional IT certifications including CISSP-ISSAP, CISSP-ISSMP, SCCP, CCSP, CISA, CRISC. He is the author of several books and has achieved many awards, including EC-Council Instructor of Excellence for 2006–07 and Top Technical Instructor Worldwide, 2002–2003. Adam earned his bachelor's degree in International Relations and his master's degree in International Political Affairs from Florida International University.

Adam has held a number of positions during his professional career including CISO, CTO, consultant, and solutions architect. He has worked on many large implementations involving multiple customer program teams for delivery.

Adam has been invited to lead projects for companies such as Microsoft, Citrix, Lloyds Bank TSB, Campus Management, US Southern Command (SOUTHCOM), Amadeus, World Fuel Services, and Seaboard Marine.

Steven Hernandez Steven Hernandez, MBA, HCISPP, CISSP, CSSLP, SSCP, CAP, CISA, is a chief information security officer practicing in the U.S. Federal Government in Washington DC. Hernandez has over 17 years of information assurance experience in a variety of fields including international healthcare, international heavy manufacturing, large finance organizations, educational institutions, and government agencies. Steven is an honorary professor at California State University – San Bernardino and affiliate faculty at the National Information Assurance Training and Education Center located at Idaho State University. Through his academic outreach, he has lectured over the past decade on numerous information assurance topics including risk management, information security investment, and the implications of privacy decisions to graduate and postgraduate audiences. In addition to his credentials from (ISC)^2, Hernandez also holds six U.S. Committee for National Security Systems certifications ranging from systems security to organizational risk management. Steven also volunteers service to (ISC)^2's Government Advisory Board and Executive Writers Bureau. Steven enjoys relaxing and traveling with his wife, whose patience and support have been indispensable in his numerous information assurance pursuits.

Credits

Project Editor
Kelly Talbot

Technical Editors
Adam Gordon
Steven Hernandez

Production Manager
Kathleen Wisor

Copy Editor
Andrew Schneiter

Manager of Content Development & Assembly
Mary Beth Wakefield

Marketing Manager
Carrie Sherrill

Professional Technology & Strategy Director
Barry Pruett

Business Manager
Amy Knies

Executive Editor
Jim Minatel

Project Coordinator, Cover
Brent Savage

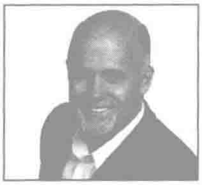
Proofreader
Kim Wimpsett

Indexer
Johnna VanHoose Dinse

Cover Designer
Mike Trent

Cover Image
Mike Trent

Foreword



CONGRATULATIONS! YOU HAVE MADE the decision to take control of your career with *The Official (ISC)^2 Guide to the SSCP CBK*. The fact that you've taken this step shows your commitment to the field and the high importance you place on continuing your professional education. It should be no surprise to you that IT professionals, who are doing hands-on work, need to be doing that work in accordance with the best practices, policies, and procedures found in the *SSCP CBK*.

This fourth edition of the *SSCP CBK* will help facilitate the practical knowledge you need to assure strong information security for your organization's daily operations. Practitioners who have proven hands-on technical ability would do well to include the *SSCP CBK* in their arsenal of tools to competently handle day-to-day responsibilities and secure their organization's data.

Reflecting the most pertinent issues that security practitioners currently face, along with the best practices for mitigating those issues, the *SSCP CBK* offers step-by-step guidance through seven domains:

- 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 the thousands of practitioners worldwide who have obtained the (ISC)^2 Systems Security Certified Practitioner (SSCP) credential. 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).

In order to meet continuing professional education requirements, SSCPs must also stay current on security issues related to changing technologies and emerging threats. As a result, SSCP practitioners can be confident that they have the know-how to competently handle day-to-day responsibilities in support of information security and business requirements.

As the recognized global leader in the field of information security education and certification, (ISC)^2's mission is to promote the development of information security professionals throughout the world. Working in coordination with members, (ISC)^2 also strives to raise the profile of the profession through security awareness programs for schoolchildren and an information security career program for colleges and their students. Earning an (ISC)^2 credential puts you in great company with a global network of professionals who echo (ISC)^2's focus to inspire a safe a secure cyber world.

As you make plans for your career, you will find that *The Official (ISC)^2 Guide to the SSCP CBK* most accurately reflects the technical and practical security knowledge required for the daily job functions of today's frontline information security practitioner.

I wish you good luck and success as you work toward achieving your goals.

Regards,

David P. Shearer, CISSP, PMP
Chief Executive Officer (CEO)
(ISC)^2

Introduction

THERE ARE TWO MAIN requirements that must be met in order to achieve the status of SSCP: one must take and pass the certification exam, and one must be able to demonstrate a minimum of one year of direct full-time security work experience in one or more of the seven domains of the (ISC)^2 SSCP CBK. A firm understanding of what the seven domains of the SSCP CBK are, and how they relate to the landscape of business, is a vital element in successfully being able to meet both requirements and claim the SSCP credential. The mapping of the seven domains of the SSCP CBK to the job responsibilities of the information security practitioner in today's world can take many paths, based on a variety of factors such as industry vertical, regulatory oversight and compliance, geography, as well as public versus private versus military as the overarching framework for employment in the first place. In addition, considerations such as cultural practices and differences in language and meaning can also play a substantive role in the interpretation of what aspects of the CBK will mean and how they will be implemented in any given workplace.

It is not the purpose of this book to attempt to address all of these issues or provide a definitive prescription as to what is "the" path forward in all areas. Rather, it is to provide the official guide to the SSCP CBK and, in so doing, to lay out the information necessary to understand what the CBK is, how it is used to build the foundation for the SSCP, and its role in business today. Being able to map the SSCP CBK to your knowledge, experience, and understanding is the way that you will be able to translate the CBK into actionable and tangible elements for both the business and its users that you represent.

1. Although **Access Control** is a single domain within the SSCP Common Body of Knowledge (CBK), it is the most pervasive and omnipresent aspect of information security. Access controls encompass all operational levels of an organization:
    - **Facilities**—Access controls protect entry to, and movement around, an organization's physical locations to protect personnel, equipment, information, and other assets inside that facility.

- **Support Systems**—Access to support systems (such as power, heating, ventilation and air conditioning [HVAC] systems; water; and fire suppression controls) must be regulated so that a malicious entity is not able to compromise these systems and cause harm to the organization's personnel or the ability to support critical systems.
- **Information Systems**—Multiple layers of access controls are present in most modern information systems and networks to protect those systems, and the information they contain, from harm or misuse.
- **Personnel**—Management, end users, customers, business partners, and nearly everyone else associated with an organization should be subject to some form of access control to ensure that the right people have the ability to interface with each other and not interfere with the people with whom they do not have any legitimate business.

The goals of information security are to ensure the continued confidentiality-integrity-availability of an organization's assets. This includes both physical assets (such as buildings, equipment, and, of course, people) and information assets (such as company data and information systems). Access controls play a key role in ensuring the confidentiality of systems and information. Managing access to physical and information assets is fundamental to preventing exposure of data by controlling who can see, use, modify, or destroy those assets. In addition, managing an entity's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated, or stolen. It is also a key factor for many organizations that are required to protect personal information in order to be compliant with appropriate legislation and industry compliance requirements.

2. The **Security Operations and Administration** domain is used to identify critical information and the execution of selected measures that eliminate or reduce adversary exploitation of critical information. It includes the definition of the controls over hardware, media, and the operators with access privileges to any of these resources. Auditing and monitoring are the mechanisms, tools, and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process. The information security practitioner should always act to maintain operational resilience, protect valuable assets, control system accounts, and manage security services effectively. In the day-to-day operations of the business, maintaining expected levels of availability and integrity for data and

services is where the information security practitioner impacts operational resilience. The day-to-day securing, monitoring, and maintenance of the resources of the business, both human and material, illustrate how the information security practitioner is able to protect valuable assets. The use of change and configuration management by the Information Security practitioner, as well as reporting and service improvement programs (SIP), ensures that the actions necessary to manage security services effectively are being carried out.

3. The **Risk Identification, Monitoring, and Analysis** domain focuses on determining system implementation and access in accordance with defined IT criteria. The use of risk management processes plays a central part in the activities of the security practitioner within this domain. Knowledge, awareness, and understanding of risk within the context of the business is an element critical to the successful implementation of an information security management system (ISMS) today, and one that this domain helps the Security Practitioner to understand and focus on. In addition, this domain also discusses collecting information for identification of, and response to, security breaches or events.
4. The **Incident Response and Recovery** domain focuses on the review, analysis, and implementation of processes essential to the identification, measurement, and control of loss associated with adverse events. The security practitioner will be expected to understand the incident handling process and how to support forensics investigations within the enterprise. In addition, knowledge of both business continuity and disaster recovery planning and processes will be important.
5. The **Cryptography** domain is a fascinating domain in the SSCP CBK. Few information security topics have the history, challenge, and technological advancements that cryptography enjoys. Throughout history, cryptography has been a crucial factor in military victories or failures, treason, espionage, and business advantage. Cryptography is both an art and a science—the use of deception and mathematics, to hide data as in steganography, to render data unintelligible through the transformation of data into an unreadable state, and to ensure that a message has not been altered in transit. Another feature of some cryptographic systems is the ability to provide assurance of who sent the message, authentication of source, and proof of delivery. Information security practitioner expectations according to the (ISC)^2 Candidate Information Bulletin are that an SSCP candidate will be expected to know basic concepts within cryptography; public and private key algorithms in terms of their applications and uses; algorithm construction, key distribution and management, and methods of attack; the

applications, construction, and use of digital signatures to provide authenticity of electronic transactions; and nonrepudiation of the parties involved.

6. The **Networks and Communication Security** domain encompasses the structures, transmission methods, transport formats, and security measures used to provide confidentiality, integrity, and availability for transmissions over private and public communications networks and media. Network security is often described as the cornerstone of IT security. The network is a central asset, if not the most central, in most IT environments. Loss of network assurance (the combined properties of confidentiality, integrity, availability, authentication, and non-repudiation) on any level can have devastating consequences, while control of the network provides an easy and consistent venue of attack. Conversely, a well-architected and well-protected network will stop many attacks in their tracks.
7. **Systems and Application Security** covers countermeasures and prevention techniques for dealing with viruses, worms, logic bombs, Trojan horses, and other related forms of intentionally damaging code. In addition, the implementation and operation of end-point device security are discussed, along with the security of big data systems. The operation and configuration of cloud computing security is a focus for the security practitioner within this domain, as is the operation and security of virtualized computing environments.

CONVENTIONS

To help you get the most from the text, we've used a number of conventions throughout the book.

REAL WORLD EXAMPLE

Real-world examples take the concepts that are being discussed and describe scenarios about how these concepts are actually handled in the real world.

✓ Try It for Yourself

These are helpful descriptions of how you can more actively put the book's concepts into actual practice.

WARNING Warnings draw attention to important information that is directly relevant to the surrounding text.

NOTE Notes discuss helpful information related to the current discussion.

As for styles in the text:

- We show URLs and code within the text like so: `persistence.properties`.
- We present code like this:

```
We use a monofont type for code examples, just as you see it in the real
world.
```

Contents