5th Edition

CISSP®

Certified Information Systems Security Professional

An (ISC)² Certification

The Official (ISC)² CISSP CBK® Reference

John Warsinske

With Mark Graff, Kevin Henry, Christopher Hoover, Ben Malisow, Sean Murphy, C. Paul Oakes, George Pajari, Jeff T. Parker, David Seidl, Mike Vasquez

SYBEX
A Wiley Brand

CISSP

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

Fifth Edition

CISSP: Certified Information Systems Security Professional

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

Fifth Edition

JOHN WARSINKSE

WITH: MARK GRAFF, KEVIN HENRY, CHRISTOPHER HOOVER, BEN MALISOW, SEAN MURPHY, C. PAUL OAKES, GEORGE PAJARI, JEFF T. PARKER, DAVID SEIDL, MIKE VASQUEZ

SYBEX
A Wiley Brand

Development Editor: Kelly Talbot
Senior Production Editor: Christine O'Connor
Copy Editor: Kim Wimpsett
Editorial Manager: Pete Gaughan
Production Manager: Kathleen Wisor
Associate Publisher: Jim Minatel
Proofreader: Louise Watson, Word One New York

Indexer: Johnna VanHoose Dinse

Project Coordinator, Cover: Brent Savage

Cover Designer: Wiley

Published simultaneously in Canada

ISBN: 978-1-119-42334-8
ISBN: 978-1-119-42332-4 (ebk.)
ISBN: 978-1-119-42331-7 (ebk.)

Manufactured in the United States of America

Library of Congress Control Number: 2019936840

10 9 8 7 6 5 4 3 2 1

Lead Author and Lead Technical Reviewer

Over the course of his 30-plus years as an information technology professional, **John Warsinske** has been exposed to a breadth of technologies and governance structures. He has been, at various times, a network analyst, IT manager, project manager, security analyst, and chief information officer. He has worked in local, state, and federal government; has worked in public, private, and nonprofit organizations; and has been variously a contractor, direct employee, and volunteer. He has served in the U.S. military in assignments at the tactical, operational, and strategic levels across the entire spectrum from peace to war. In these diverse environments, he has experienced both the uniqueness and the similarities in the activities necessary to secure their respective information assets.

Mr. Warsinske has been an instructor for $(ISC)^2$ for more than five years; prior to that, he was an adjunct faculty instructor at the College of Southern Maryland. His $(ISC)^2$ certifications include the Certified Information Systems Security Professional (CISSP), Certified Cloud-Security Professional (CCSP), and HealthCare Information Security and Privacy Practitioner (HCISPP). He maintains several other industry credentials as well.

When he is not traveling, Mr. Warsinske currently resides in Ormond Beach, Florida, with his wife and two extremely spoiled Carolina dogs.

Contributing Authors

Mark Graff (CISSP), former chief information security officer for both NASDAQ and Lawrence Livermore National Laboratory, is a seasoned cybersecurity practitioner and thought leader. He has lectured on risk analysis, cybersecurity, and privacy issues before the American Academy for the Advancement of Science, the Federal Communications Commission, the Pentagon, the National Nuclear Security Administration, and other U.S. national security facilities. Graff has twice testified before Congress on cybersecurity, and in 2018–2019 served as an expert witness on software security to the Federal Trade Commission. His books—notably *Secure Coding: Principles and Practices*—have been used at dozens of universities worldwide in teaching how to design and build secure software-based systems. Today, as head of the consulting firm Tellagraff LLC (`www.markgraff.com`), Graff provides strategic advice to large companies, small businesses, and government agencies. Recent work has included assisting multiple state governments in the area of election security.

Kevin Henry (CAP, CCSP, CISSP, CISSP-ISSAP, CISSP-ISSEP, CISSP-ISSMP, CSSLP, and SSCP) is a passionate and effective educator and consultant in information security. Kevin has taught CISSP classes around the world and has contributed to the development of $(ISC)^2$ materials for nearly 20 years. He is a frequent speaker at security conferences and the author of several books on security management. Kevin's years of work in telecommunications, government, and private industry have led to his strength in being able to combine real-world experience with the concepts and application of information security topics in an understandable and effective manner.

Chris Hoover, CISSP, CISA, is a cybersecurity and risk management professional with 20 years in the field. He spent most of his career protecting the U.S. government's most sensitive data in the Pentagon, the Baghdad Embassy, NGA Headquarters, Los Alamos Labs, and many other locations. Mr. Hoover also developed security products for RSA that are deployed across the U.S. federal government, many state governments, and internationally. He is currently consulting for the DoD and runs a risk management start-up called Riskuary. He has a master's degree in information assurance.

Ben Malisow, CISSP, CISM, CCSP, Security+, SSCP, has been involved in INFOSEC and education for more than 20 years. At Carnegie Mellon University, he crafted and delivered the CISSP prep course for CMU's CERT/SEU. Malisow was the ISSM for the FBI's most highly classified counterterror intelligence-sharing network, served as an Air Force officer, and taught grades 6–12 at a reform school in the Las Vegas public school district (probably his most dangerous employment to date). His latest work has included *CCSP Practice Tests* and *CCSP (ISC)² Certified Cloud Security Professional Official Study Guide*, also from Sybex/Wiley, and *How to Pass Your INFOSEC Certification Test: A Guide to Passing the CISSP, CISA, CISM, Network+, Security+, and CCSP*, available from Amazon Direct. In addition to other consulting and teaching, Ben is a certified instructor for (ISC)², delivering CISSP, CCSP, and SSCP courses. You can reach him at `www.benmalisow.com` or his INFOSEC blog, `securityzed.com`. Ben would also like to extend his personal gratitude to Todd R. Slack, MS, JD, CIPP/US, CIPP/E, CIPM, FIP, CISSP, for his invaluable contributions to this book.

Sean Murphy, CISSP, HCISSP, is the vice president and chief information security officer for Premera Blue Cross (Seattle). He is responsible for providing and optimizing an enterprise-wide security program and architecture that minimizes risk, enables business imperatives, and further strengthens the health plan company's security posture. He's a healthcare information security expert with more than 20 years of experience in highly regulated, security-focused organizations. Sean retired from the U.S. Air Force (Medical Service Corps) after achieving the rank of lieutenant colonel. He has served as CIO and CISO in the military service and private sector at all levels of healthcare organizations. Sean has a master's degree in business administration (advanced IT concentration) from the University of South Florida, a master's degree in health services administration from Central Michigan University, and a bachelor's degree in human resource management from the University of Maryland. He is a board chair of the Association for Executives in Healthcare Information Security (AEHIS). Sean is a past chairman of the HIMSS Privacy and Security Committee. He served on the (ISC)² committee to develop the HCISPP credential. He is also a noted speaker at the national level and the author of numerous industry whitepapers, articles, and educational materials, including his book *Healthcare Information Security and Privacy*.

C. Paul Oakes, CISSP, CISSP-ISSAP, CCSP, CCSK, CSM, and CSPO, is an author, speaker, educator, technologist, and thought leader in cybersecurity, software development, and process improvement. Paul has worn many hats over his 20-plus years of experience. In his career he has been a security architect, consultant, software engineer, mentor, educator, and executive. Paul has worked with companies in various industries such as the financial industry, banking, publishing, utilities, government, e-commerce, education, training, research, and technology start-ups. His work has advanced the cause of software and information security on many fronts, ranging from writing security policy to implementing secure code and showing others how to do the same. Paul's passion is to help people develop the skills they need to most effectively defend the line in cyberspace and advance the standard of cybersecurity practice. To this end, Paul continuously collaborates with experts across many disciplines, ranging from cybersecurity to accelerated learning to mind-body medicine, to create and share the most effective strategies to rapidly learn cybersecurity and information technology subject matter. Most of all, Paul enjoys his life with his wife and young son, both of whom are the inspirations for his passion.

George E. Pajari, CISSP-ISSAP, CISM, CIPP/E, is a fractional CISO, providing cybersecurity leadership on a consulting basis to a number of cloud service providers. Previously he was the chief information security officer (CISO) at Hootsuite, the most widely used social media management platform, trusted by more than 16 million people and employees at 80 percent of the Fortune 1000. He has presented at conferences including CanSecWest, ISACA CACS, and BSides Vancouver. As a volunteer, he helps with the running of BSides Vancouver, the (ISC)² Vancouver chapter, and the University of British Columbia's Cybersecurity Summit. He is a recipient of the ISACA CISM Worldwide Excellence Award.

Jeff Parker, CISSP, CySA+, CASP, is a certified technical trainer and security consultant specializing in governance, risk management, and compliance (GRC). Jeff began his information security career as a software engineer with an HP consulting group out of Boston. Enterprise clients for which Jeff has consulted on site include hospitals, universities, the U.S. Senate, and a half-dozen UN agencies. Jeff assessed these clients' security posture and provided gap analysis and remediation. In 2006 Jeff relocated to Prague, Czech Republic, for a few years, where he designed a new risk management strategy for a multinational logistics firm. Presently, Jeff resides in Halifax, Canada, while consulting primarily for a GRC firm in Virginia.

David Seidl, CISSP, GPEN, GCIH, CySA+, Pentest+, is the vice president for information technology and CIO at Miami University of Ohio. During his IT career, he has served in a variety of technical and information security roles, including serving as the senior director for Campus Technology Services at the University of Notre Dame and leading Notre Dame's information security team as director of information security. David has taught college courses on information security and writes books on information security and cyberwarfare, including *CompTIA CySA+ Study Guide: Exam CS0-001*, *CompTIA PenTest+ Study Guide: Exam PT0-001*, *CISSP Official (ISC)² Practice Tests*, and *CompTIA CySA+ Practice Tests: Exam CS0-001*, all from Wiley, and *Cyberwarfare: Information Operations in a Connected World* from Jones and Bartlett. David holds a bachelor's degree in communication technology and a master's degree in information security from Eastern Michigan University.

Michael Neal Vasquez has more than 25 years of IT experience and has held several industry certifications, including CISSP, MCSE: Security, MCSE+I, MCDBA, and CCNA. Mike is a senior security engineer on the red team for a Fortune 500 financial services firm, where he spends his days (and nights) looking for security holes. After obtaining his BA from Princeton University, he forged a security-focused IT career, both working in the trenches and training other IT professionals. Mike is a highly sought-after instructor because his classes blend real-world experience and practical knowledge with the technical information necessary to comprehend difficult material, and his students praise his ability to make any course material entertaining and informative. Mike has taught CISSP, security, and Microsoft to thousands of students across the globe through local colleges and online live classes. He has performed penetration testing engagements for healthcare, financial services, retail, utilities, and government entities. He also runs his own consulting and training company and can be reached on LinkedIn at `https://www.linkedin.com/in/mnvasquez`.

Technical Reviewers

Bill Burke, CISSP, CCSP, CRISC, CISM, CEH, is a security professional with more than 35 years serving the information technology and services community. He specializes in security architecture, governance, and compliance, primarily in the cloud space. He previously served on the board of directors of the Silicon Valley (ISC)^2 chapter, in addition to the board of directors of the Cloud Services Alliance – Silicon Valley. Bill can be reached via email at `billburke@cloudcybersec.com`.

Charles Gaughf, CISSP, SSCP, CCSP, is both a member and an employee of (ISC)^2, the global nonprofit leader in educating and certifying information security professionals. For more than 15 years, he has worked in IT and security in different capacities for nonprofit, higher education, and telecommunications organizations to develop security education for the industry at large. In leading the security team for the last five years as the senior manager of security at (ISC)^2, he was responsible for the global security operations, security posture, and overall security health of (ISC)^2. Most recently he transitioned to the (ISC)^2 education team to develop immersive and enriching CPE opportunities and security training and education for the industry at large. He holds degrees in management of information systems and communications.

Dr. Meng-Chow Kang, CISSP, is a practicing information security professional with more than 30 years of field experience in various technical information security and risk management roles for organizations that include the Singapore government, major global financial institutions, and security and technology providers. His research and part of his experience in the field have been published in his book *Responsive Security: Be Ready to Be Secure* from CRC Press. Meng-Chow has been a CISSP since 1998 and was a member of the (ISC)^2 board of directors from 2015 through 2017. He is also a recipient of the (ISC)^2 James Wade Service Award.

Aaron Kraus, CISSP, CCSP, Security+, began his career as a security auditor for U.S. federal government clients working with the NIST RMF and Cybersecurity Framework, and then moved to the healthcare industry as an auditor working with the HIPAA and HITRUST frameworks. Next, he entered the financial services industry, where he designed a control and audit program for vendor risk management, incorporating financial compliance requirements and industry-standard frameworks including COBIT and ISO 27002. Since 2016 Aaron has been working with startups based in San Francisco, first on a GRC SaaS platform and more recently in cyber-risk insurance, where he focuses on assisting small- to medium-sized businesses to identify their risks, mitigate them appropriately, and transfer risk via insurance. In addition to his technical certifications, he is a Learning Tree certified instructor who teaches cybersecurity exam prep and risk management.

Professor Jill Slay, CISSP, CCFP, is the optus chair of cybersecurity at La Trobe University, leads the Optus La Trobe Cyber Security Research Hub, and is the director of cyber-resilience initiatives for the Australian Computer Society. Jill is a director of the Victorian Oceania Research Centre and previously served two terms as a director of the International Information Systems Security Certification Consortium. She has established an international research reputation in cybersecurity (particularly digital forensics) and has worked in collaboration with many industry partners. She was made a member of the Order of Australia (AM) for service to the information technology industry through contributions in the areas of forensic computer science, security, protection of infrastructure, and cyberterrorism. She is a fellow of the Australian Computer Society and a fellow of the International Information Systems Security Certification Consortium, both for her service to the information security industry. She also is a MACS CP.

Contents at a Glance

Contents

Foreword

BEING RECOGNIZED AS A CISSP is an important step in investing in your information security career. Whether you are picking up this book to supplement your preparation to sit for the exam or you are an existing CISSP using this as a desk reference, you've acknowledged that this certification makes you recognized as one of the most respected and sought-after cybersecurity leaders in the world. After all, that's what the CISSP symbolizes. You and your peers are among the ranks of the most knowledgeable practitioners in our community. The designation of CISSP instantly communicates to everyone within our industry that you are intellectually curious and traveling along a path of lifelong learning and improvement. Importantly, as a member of (ISC)² you have officially committed to ethical conduct commensurate to your position of trust as a cybersecurity professional.

The recognized leader in the field of information security education and certification, (ISC)² promotes the development of information security professionals throughout the world. As a CISSP with all the benefits of (ISC)² membership, you are part of a global network of more than 140,000 certified professionals who are working to inspire a safe and secure cyber world.

Being a CISSP, though, is more than a credential; it is what you demonstrate daily in your information security role. The value of your knowledge is the proven ability to effectively design, implement, and manage a best-in-class cybersecurity program within your organization. To that end, it is my great pleasure to present the *Official (ISC)² Guide to the CISSP (Certified Information Systems Security Professional) CBK*. Drawing from a comprehensive, up-to-date global body of knowledge, the *CISSP CBK* provides you with valuable insights on how to implement every aspect of cybersecurity in your organization.

If you are an experienced CISSP, you will find this edition of the *CISSP CBK* to be a timely book to frequently reference for reminders on best practices. If you are still gaining the experience and knowledge you need to join the ranks of CISSPs, the *CISSP CBK* is a deep dive that can be used to supplement your studies.

As the largest nonprofit membership body of certified information security professionals worldwide, (ISC)² recognizes the need to identify and validate not only information security competency but also the ability to connect knowledge of several domains when building high-functioning cybersecurity teams that demonstrate cyber resiliency. The CISSP credential represents advanced knowledge and competency in security design, implementation, architecture, operations, controls, and more.

If you are leading or ready to lead your security team, reviewing the *Official (ISC)^2 Guide to the CISSP CBK* will be a great way to refresh your knowledge of the many factors that go into securely implementing and managing cybersecurity systems that match your organization's IT strategy and governance requirements. The goal for CISSP credential holders is to achieve the highest standard for cybersecurity expertise—managing multiplatform IT infrastructures while keeping sensitive data secure. This becomes especially crucial in the era of digital transformation, where cybersecurity permeates virtually every value stream imaginable. Organizations that can demonstrate world-class cybersecurity capabilities and trusted transaction methods can enable customer loyalty and fuel success.

The opportunity has never been greater for dedicated men and women to carve out a meaningful career and make a difference in their organizations. The *CISSP CBK* will be your constant companion in protecting and securing the critical data assets of your organization that will serve you for years to come.

Regards,

David P. Shearer, CISSP
CEO, (ISC)^2

Introduction

THE CERTIFIED INFORMATION SYSTEMS Security Professional (CISSP) signifies that an individual has a cross-disciplinary expertise across the broad spectrum of information security and that he or she understands the context of it within a business environment. There are two main requirements that must be met in order to achieve the status of CISSP. One must take and pass the certification exam, while also proving a minimum of five years of direct full-time security work experience in two or more of the domains of the (ISC)² CISSP CBK. The field of information security is wide, and there are many potential paths along one's journey through this constantly and rapidly changing profession.

A firm comprehension of the domains within the CISSP CBK and an understanding of how they connect back to the business and its people are important components in meeting the requirements of the CISSP credential. Every reader will connect these domains to their own background and perspective. These connections will vary based on industry, regulatory environment, geography, culture, and unique business operating environment. With that sentiment in mind, this book's purpose is not to address all of these issues or prescribe a set path in these areas. Instead, the aim is to provide an official guide to the CISSP CBK and allow you, as a security professional, to connect your own knowledge, experience, and understanding to the CISSP domains and translate the CBK into value for your organization and the users you protect.

SECURITY AND RISK MANAGEMENT

The Security and Risk Management domain entails many of the foundational security concepts and principles of information security. This domain covers a broad set of topics and demonstrates how to generally apply the concepts of confidentiality, integrity and availability across a security program. This domain also includes understanding compliance requirements, governance, building security policies and procedures, business continuity planning, risk management, security education, and training and awareness, and most importantly it lays out the ethnical canons and professional conduct to be demonstrated by (ISC)² members.

The information security professional will be involved in all facets of security and risk management as part of the functions they perform across the enterprise. These functions may include developing and enforcing policy, championing governance and risk management, and ensuring the continuity of operations across an organization in the event of unforeseen circumstances. To that end, the information security professional must safeguard the organization's people and data.

ASSET SECURITY

The Asset Security domain covers the safeguarding of information and information assets across their lifecycle to include the proper collection, classification, handling, selection, and application of controls. Important concepts within this domain are data ownership, privacy, data security controls, and cryptography. Asset security is used to identify controls for information and the technology that supports the exchange of that information to include systems, media, transmission, and privilege.

The information security professional is expected to have a solid understanding of what must be protected, what access should be restricted, the control mechanisms available, how those mechanisms may be abused, and the appropriateness of those controls, and they should be able to apply the principles of confidentiality, integrity, availability, and privacy against those assets.

SECURITY ARCHITECTURE AND ENGINEERING

The Security Architecture and Engineering domain covers the process of designing and building secure and resilient information systems and associated architecture so that the information systems can perform their function while minimizing the threats that can be caused by malicious actors, human error, natural disasters, or system failures. Security must be considered in the design, in the implementation, and during the continuous delivery of an information system through its lifecycle. It is paramount to understand secure design principles and to be able to apply security models to a wide variety of distributed and disparate systems and to protect the facilities that house these systems.

An information security professional is expected to develop designs that demonstrate how controls are positioned and how they function within a system. The security controls must tie back to the overall system architecture and demonstrate how, through security engineering, those systems maintain the attributes of confidentiality, integrity, and availability.

COMMUNICATION AND NETWORK SECURITY

The Communication and Network Security domain covers secure design principles as they relate to network architectures. The domain provides a thorough understanding of components of a secure network, secure design, and models for secure network operation. The domain covers aspects of a layered defense, secure network technologies, and management techniques to prevent threats across a number of network types and converged networks.

It is necessary for an information security professional to have a thorough understanding of networks and the way in which organizations communicate. The connected world in which security professionals operate requires that organizations be able to access information and execute transactions in real time with an assurance of security. It is therefore important that an information security professional be able to identify threats and risks and then implement mitigation techniques and strategies to protect these communication channels.

IDENTITY AND ACCESS MANAGEMENT (IAM)

The Identity and Access Management (IAM) domain covers the mechanisms by which an information system permits or revokes the right to access information or perform an action against an information system. IAM is the mechanism by which organizations manage digital identities. IAM also includes the organizational policies and processes for managing digital identities as well as the underlying technologies and protocols needed to support identity management.

Information security professionals and users alike interact with components of IAM every day. This includes business services logon authentication, file and print systems, and nearly any information system that retrieves and manipulates data. This can mean users or a web service that exposes data for user consumption. IAM plays a critical and indispensable part in these transactions and in determining whether a user's request is validated or disqualified from access.

SECURITY ASSESSMENT AND TESTING

The Security Assessment and Testing domain covers the tenets of how to perform and manage the activities involved in security assessment and testing, which includes providing a check and balance to regularly verify that security controls are performing optimally and efficiently to protect information assets. The domain describes the array of tools and methodologies for performing various activities such as vulnerability assessments, penetration tests, and software tests.