(ISC)²®

Second Edition

THE OFFICIAL (ISC)²® GUIDE TO THE CCSP℠ CBK®

Gordon

» Produced by (ISC)², the trusted source of industry expertise for cyber, information, software and infrastructure security

» The definitive "common" body of knowledge used by candidates for the Certified Cloud Security Professional (CCSP) credential

CCSP℠

Certified Cloud Security Professional

SYBEX
A Wiley Brand

The Official (ISC)²® Guide to the CCSP℠ CBK®

Second Edition

ADAM GORDON
CISSP-ISSAP, CISSP-ISSMP, SSCP, CCSP, CISA,
CRISC, MCSE PRIVATE CLOUD, VCP-CLOUD

(ISC)²

SYBEX
A Wiley Brand

The Official (ISC)2® Guide to the CCSP℠ CBK®, Second 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: 978-1-119-27672-2
ISBN: 978-1-119-27673-9 (ebk)
ISBN: 978-1-119-27674-6 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Library of Congress Control Number: 2016935632

About the Author

With more than 25 years of experience as both an educator and an IT professional, Adam Gordon holds numerous professional IT certifications, including CISSP, CISA, CRISC, CHFI, CEH, SCNA, VCP, and VCI. He is the author of several books and has earned numerous awards, including EC-Council Instructor of Excellence, 2006 -2007 and Top Technical Instructor Worldwide, 2002 -2003. Adam holds 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.

Credits

Project Editors
Gill Editorial Services
Kelly Talbot

Technical Editor
Rob Shimonski

Production Manager
Kathleen Wisor

Copy Editor
Kezia Endsley

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

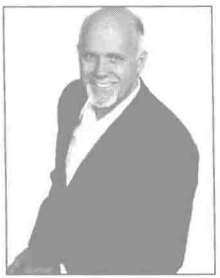
Proofreader
Kim Wimpsett

Indexer
Johnna VanHoose Dinse

Cover Designer
Mike Trent

Cover Image
Mike Trent

Foreword



EVERY DAY AROUND THE WORLD, organizations are taking steps to leverage cloud infrastructure, software, and services. This is a substantial undertaking that also heightens the complexity of protecting and securing data. As powerful as cloud computing is to organizations, it's essential to have qualified people who understand information security risks and mitigation strategies for the cloud. As the largest not-for-profit membership body of certified information security professionals worldwide, (ISC)^2 recognizes the need to identify and validate information security competency in securing cloud services.

To help facilitate the knowledge you need to ensure strong information security in the cloud, I'm pleased to present the *Official (ISC)^2 Guide to the CCSP CBK*. Drawing from a comprehensive, up-to-date global body of knowledge, the *CCSP CBK* ensures that you have the right information security knowledge and skills to be successful and prepares you to achieve the Certified Cloud Security Professional (CCSP) credential.

(ISC)^2 is proud to collaborate with the Cloud Security Alliance (CSA) to build a unique credential that reflects the most current and comprehensive best practices for securing and optimizing cloud computing environments. To attain CCSP certification, candidates must have a minimum of five years' experience in IT, of which three years must be in information security and one year in cloud computing. All CCSP candidates must be able to demonstrate capabilities found in each of the six Common Body of Knowledge (CBK) domains:

- Architectural Concepts and Design Requirements
- Cloud Data Security
- Cloud Platform and Infrastructure Security

- Cloud Application Security
- Operations
- Legal and Compliance

The CCSP credential represents advanced knowledge and competency in cloud security design, implementation, architecture, operations, controls, and immediate and long-term responses.

Cloud computing has emerged as a critical area within IT that requires further security considerations. According to the 2015 (ISC)² Global Information Security Workforce Study, cloud computing is identified as the top area for information security, with a growing demand for education and training within the next three years. In correlation to the demand for education and training, 73 percent of more than 13,000 survey respondents believe that cloud computing will require information security professionals to develop new skills.

If you are ready to take control of the cloud, *The Official (ISC)² Guide to the CCSP CBK* prepares you to securely implement and manage cloud services within your organization's information technology (IT) strategy and governance requirements. CCSP credential holders will achieve the highest standard for cloud security expertise—managing the power of cloud computing while keeping sensitive data secure.

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 CCSP with all the benefits of (ISC)² membership, you would join a global network of more than 110,000 certified professionals who are working to inspire a safe and secure cyber world.

Qualified people are the key to cloud security. This is your opportunity to gain the knowledge and skills you need to protect and secure data in the cloud.

Regards,

David P. Shearer
CEO
(ISC)²

Introduction

THERE ARE TWO MAIN requirements that must be met to achieve the status of Certified Cloud Security Professional (CCSP); one must take and pass the certification exam and be able to demonstrate a minimum of five years of cumulative paid full-time information technology experience, of which three years must be in information security and one year must be in one of the six domains of the CCSP examination. A firm understanding of what the six domains of the CCSP Common Body of Knowledge (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 CCSP credential. The mapping of the six domains of the CCSP CBK to the job responsibilities of the information security professional in today's world can take many paths based on a variety of factors, such as industry vertical, regulatory oversight and compliance, geography, and 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 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 these issues or provide a definitive prescription as to "the" path forward in all areas. Rather, it is to provide the official guide to the CCSP CBK and, in so doing, to lay out the information necessary to understand what the CBK is and how it is used to build the foundation for the CCSP and its role in business today. Being able to map the CCSP 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. The Architectural Concepts and Design Requirements domain focuses on the building blocks of cloud-based systems. The CCSP needs an understanding of cloud computing concepts such as definitions based on the ISO/IEC 17788 standard; roles like the cloud service customer, provider, and partner; characteristics such as multitenancy, measured services, and rapid elasticity and scalability; and building block technologies of the cloud such as virtualization, storage, and networking. The cloud reference architecture will

need to be described and understood, focusing on areas such as cloud computing activities (as described in ISO/IEC 17789), clause 9, cloud service capabilities, categories, deployment models, and the cross-cutting aspects of cloud platform architecture and design, such as interoperability, portability, governance, service levels, and performance. In addition, the CCSP should have a clear understanding of the relevant security and design principles for cloud computing, such as cryptography, access control, virtualization security, functional security requirements like vendor lock-in and interoperability, what a secure data life cycle is for cloud-based data, and how to carry out a cost-benefit analysis of cloud-based systems. The ability to identify what a trusted cloud service is and what role certification against criteria plays in that identification—using standards such as the Common Criteria and FIPS 140-2—are further areas of focus for this domain.

2. The Cloud Data Security domain contains the concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems (OSs), equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability. The CCSP needs to understand and implement data discovery and classification technologies pertinent to cloud platforms, as well as be able to design and implement relevant jurisdictional data protections for personally identifiable information (PII), such as data privacy acts and the ability to map and define controls within the cloud. Designing and implementing digital rights management (DRM) solutions with the appropriate tools and planning for the implementation of data retention, deletion, and archiving policies are activities that a CCSP will need to understand how to undertake.
3. The Cloud Platform and Infrastructure Security domain covers knowledge of the cloud infrastructure components—both the physical and virtual—existing threats, and mitigating and developing plans to deal with those threats. Risk management is the identification, measurement, and control of loss associated with adverse events. It includes overall security review, risk analysis, selection and evaluation of safeguards, cost-benefit analysis, management decisions, safeguard implementation, and effectiveness review. The CCSP is expected to understand risk management, including risk analysis, threats and vulnerabilities, asset identification, and risk management tools and techniques. In addition, the candidate needs to understand how to design and plan for the use of security controls such as audit mechanisms, physical and environmental protection, and the management of identification, authentication, and authorization solutions within the cloud infrastructures she manages. Business continuity planning (BCP) facilitates the rapid recovery of business operations to reduce the overall impact of the disaster by ensuring continuity of the critical business functions. Disaster recovery planning includes procedures for emergency response, extended backup operations, and postdisaster recovery when the computer installation suffers loss of computer resources and physical facilities. The CCSP is expected to understand how to prepare a business continuity or disaster recovery plan (DRP), techniques and concepts, identification of critical data and systems, and the recovery of lost data within cloud infrastructures.

4. The Cloud Application Security domain focuses on issues to ensure that the need for training and awareness in application security, the processes involved with cloud software assurance and validation, and the use of verified secure software are understood. The domain refers to the controls that are included within systems and applications software and the steps used in their development (such as software development life cycle). The CCSP should fully understand the security and controls of the development process, system life cycle, application controls, change controls, program interfaces, and concepts used to ensure data and application integrity, security, and availability. In addition, the need to understand how to design appropriate identity and access management (IAM) solutions for cloud-based systems is important.
5. The Operations domain is used to identify critical information and the execution of selected measures that eliminate or reduce adversary exploitation of critical information. The domain examines the requirements of the cloud architecture, from planning of the data center design and implementation of the physical and logical infrastructure for the cloud environment to running and managing that infrastructure. 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 understanding of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process. The need for compliance with regulations and controls through the applications of frameworks such as ITIL and ISO/IEC 20000 is also discussed. In addition, the importance of risk assessment across both the logical and the physical infrastructures and the management of communication with all relevant parties are focused on. The CCSP is expected to know the resources that must be protected, the privileges that must be restricted, the control mechanisms that are available, the potential for abuse of access, the appropriate controls, and the principles of good practice.
6. The Legal and Compliance domain addresses ethical behavior and compliance with regulatory frameworks. It includes the investigative measures and techniques that can be used to determine if a crime has been committed and methods used to gather evidence (including legal controls, e-discovery, and forensics). This domain also includes an understanding of privacy issues and audit processes and methodologies required for a cloud environment, such as internal and external audit controls, assurance issues associated with virtualization and the cloud, and the types of audit reporting specific to the cloud, such as the Statement on Standards for Attestation Engagements (SSAE) No. 16, and the International Standards for Assurance Engagements (ISAE) No. 3402.[1] Further, examining and understanding the implications that cloud environments have in relation to enterprise risk management and the impact of outsourcing for design and hosting of these systems are important considerations that many organizations face today.

[1] Many service organizations that previously had a SAS 70 service auditor's examination (SAS 70 audit) performed converted to the SSAE No.16 standard in 2011 and now have an SSAE 16 report instead. This is also referred to as a Service Organization Controls (SOC) 1 report.

CONVENTIONS

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

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 within the text like so: `www.wiley.com`.

Contents