

(ISC)²®

Second Edition

THE OFFICIAL (ISC)²® GUIDE TO THE
CCSPSM 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



Certified Cloud
Security Professional

SYBEX
A Wiley Brand

The Official (ISC)²[®] Guide to the CCSPSM 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 CCSPSM CBK[®], Second Edition

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

Copyright © 2016 by (ISC)²®

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

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 Sections 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, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. 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/permissions>.

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 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: 2016935632

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, CCSP, and CBK are service marks or registered trademarks of Information System Security 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.

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

Foreword	xvii
Introduction	xix
DOMAIN 1: ARCHITECTURAL CONCEPTS AND DESIGN REQUIREMENTS	1
Introduction	3
Drivers for Cloud Computing	4
Security, Risks, and Benefits	5
Cloud Computing Definitions	7
Cloud Computing Roles	12
Key Cloud Computing Characteristics	12
Cloud Transition Scenario	14
Building Blocks	16
Cloud Computing Functions	16
Cloud Service Categories	18
IaaS	18
PaaS	19
SaaS	21
Cloud Deployment Models	23
The Public Cloud Model	23
The Private Cloud Model	23
The Hybrid Cloud Model	24
The Community Cloud Model	25
Cloud Cross-Cutting Aspects	25
Architecture Overview	25
Key Principles of an Enterprise Architecture	27
The NIST Cloud Technology Roadmap	28
Network Security and Perimeter	32
Cryptography	33
Encryption	33
Key Management	35

IAM and Access Control	37
Provisioning and Deprovisioning	37
Centralized Directory Services	38
Privileged User Management	38
Authorization and Access Management	39
Data and Media Sanitization	40
Vendor Lock-In	40
Cryptographic Erasure	41
Data Overwriting	41
Virtualization Security	42
The Hypervisor	42
Security Types	43
Common Threats	43
Data Breaches	43
Data Loss	44
Account or Service Traffic Hijacking	45
Insecure Interfaces and APIs	45
Denial of Service	46
Malicious Insiders	46
Abuse of Cloud Services	46
Insufficient Due Diligence	47
Shared Technology Vulnerabilities	47
Security Considerations for Different Cloud Categories	48
IaaS Security	48
PaaS Security	50
SaaS Security	52
Open Web Application Security Project Top Ten Security Threats	54
Cloud Secure Data Lifecycle	55
Information and Data Governance Types	56
Business Continuity and Disaster Recovery Planning	57
Business Continuity Elements	57
Critical Success Factors	58
Important SLA Components	59
Cost-Benefit Analysis	60
Certification Against Criteria	62
System and Subsystem Product Certification	69
Summary	72
Review Questions	73
Notes	77

DOMAIN 2: CLOUD DATA SECURITY	79
Introduction	81
The Cloud Data Lifecycle Phases	82
Location and Access of Data	83
Location	83
Access	84
Functions, Actors, and Controls of the Data	84
Key Data Functions	85
Controls	85
Process Overview	86
Tying It Together	86
Cloud Services, Products, and Solutions	87
Data Storage	87
IaaS	87
PaaS	88
SaaS	89
Threats to Storage Types	90
Technologies Available to Address Threats	91
Relevant Data Security Technologies	91
Data Dispersion in Cloud Storage	92
DLP	92
Encryption	95
Masking, Obfuscation, Anonymization, and Tokenization	102
Application of Security Strategy Technologies	105
Emerging Technologies	106
Bit Splitting	106
Homomorphic Encryption	107
Data Discovery	108
Data Discovery Approaches	108
Different Data Discovery Techniques	109
Data Discovery Issues	110
Challenges with Data Discovery in the Cloud	111
Data Classification	112
Data Classification Categories	112
Challenges with Cloud Data	113
Data Privacy Acts	113
Global P&DP Laws in the United States	114
Global P&DP Laws in the European Union	115
Global P&DP Laws in APEC	115
Differences Between Jurisdiction and Applicable Law	115
Essential Requirements in P&DP Laws	116

Typical Meanings for Common Privacy Terms	116
Privacy Roles for Customers and Service Providers	117
Responsibility Depending on the Type of Cloud Services	118
Implementation of Data Discovery	119
Classification of Discovered Sensitive Data	120
Mapping and Definition of Controls	123
Privacy Level Agreement	124
PLA Versus Essential P&DP Requirements Activity	124
Application of Defined Controls for PII	128
Cloud Security Alliance Cloud Controls Matrix	129
Management Control for Privacy and Data-Protection Measures	133
Data Rights Management Objectives	134
IRM Cloud Challenges	134
IRM Solutions	135
Data-Protection Policies	136
Data-Retention Policies	137
Data-Deletion Procedures and Mechanisms	138
Data-Archiving Procedures and Mechanisms	139
Events	140
Event Sources	140
Identifying Event Attribute Requirements	142
Storage and Analysis of Data Events	144
SIEM	145
Supporting Continuous Operations	146
Chain of Custody and Nonrepudiation	147
Summary	148
Review Questions	149
Notes	152
DOMAIN 3: CLOUD PLATFORM AND INFRASTRUCTURE	
SECURITY	155
Introduction	157
The Physical Environment of the Cloud Infrastructure	157
Data Center Design	158
Network and Communications in the Cloud	159
Network Functionality	159
Software-Defined Networking	160
The Compute Parameters of a Cloud Server	161
Virtualization	161
Scalability	162
The Hypervisor	162

Storage Issues in the Cloud	163
Object Storage	164
Management Plane	164
Management of Cloud Computing Risks	166
Risk Assessment and Analysis	166
Cloud Attack Vectors	170
Countermeasure Strategies Across the Cloud	170
Continuous Uptime	171
Automation of Controls	171
Access Controls	171
Physical and Environmental Protections	172
Key Regulations	173
Examples of Controls	173
Protecting Data Center Facilities	173
System and Communication Protections	173
Automation of Configuration	174
Responsibilities of Protecting the Cloud System	174
Following the Data Lifecycle	175
Virtualization Systems Controls	176
Managing Identification, Authentication, and Authorization in the Cloud Infrastructure	178
Managing Identification	178
Managing Authentication	179
Managing Authorization	179
Accounting for Resources	179
Managing Identity and Access Management	179
Making Access Decisions	179
The Entitlement Process	180
The Access Control Decision-Making Process	180
Risk Audit Mechanisms	181
The Cloud Security Alliance Cloud Controls Matrix	182
Cloud Computing Audit Characteristics	182
Using a VM	183
Understanding the Cloud Environment Related to BCDR	183
On-Premises, Cloud as BCDR	184
Cloud Service Consumer, Primary Provider BCDR	184
Cloud Service Consumer, Alternative Provider BCDR	185
BCDR Planning Factors	185
Relevant Cloud Infrastructure Characteristics	185
Understanding the Business Requirements Related to BCDR	186
Understanding the BCDR Risks	188
BCDR Risks Requiring Protection	188
BCDR Strategy Risks	188
Potential Concerns About the BCDR Scenarios	189

BCDR Strategies	190
Location	191
Data Replication	191
Functionality Replication	192
Planning, Preparing, and Provisioning	192
Failover Capability	192
Returning to Normal	193
Creating the BCDR Plan	193
The Scope of the BCDR Plan	193
Gathering Requirements and Context	193
Analysis of the Plan	194
Risk Assessment	194
Plan Design	194
Other Plan Considerations	195
Planning, Exercising, Assessing, and Maintaining the Plan	195
Test Plan Review	197
Testing and Acceptance to Production	201
Summary	201
Review Questions	202
Notes	204
DOMAIN 4: CLOUD APPLICATION SECURITY	205
Introduction	207
Determining Data Sensitivity and Importance	208
Understanding the API Formats	208
Common Pitfalls of Cloud Security Application Deployment	209
On-Premises Does Not Always Transfer (and Vice Versa)	210
Not All Apps Are Cloud Ready	210
Lack of Training and Awareness	210
Lack of Documentation and Guidelines	211
Complexities of Integration	211
Overarching Challenges	211
Awareness of Encryption Dependencies	213
Understanding the Software Development Lifecycle Process	
for a Cloud Environment	213
Secure Operations Phase	214
Disposal Phase	215
Assessing Common Vulnerabilities	215
Cloud-Specific Risks	218
Threat Modeling	220
STRIDE Threat Model	220
Approved Application Programming Interfaces	221