ISC2 Certified Cloud Security Professional (CCSP) Exam Guide

Essential strategies for compliance, governance, and risk management

Kim van Lavieren

www.bpbonline.com

First Edition 2024

ISBN: 978-93-55517-654

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

Dedicated to

My loving wife:

Sarah van Lavieren

&

My grandparents:

Fred *and* ***Ada***

About the Author

Kim van Lavieren is currently a managing consultant at SimplifyNow. Throughout his career, he has helped many organizations bolster their security. His experience ranges from security engineering (at a FANG company) to architecture to the boardroom as a CISO. He holds an MSc in cybersecurity and a BSc in software engineering. Throughout his career, he has obtained a wide variety of (cloud) security certifications, including (but not limited to): CCSP, CISSP, CISM, CISSP-ISSEP, CISSP-ISSAP, CISSP-ISSMP, CSSLP, CGRC, Microsoft Certified: Cybersecurity Architect Expert, and the AWS Security Specialty.

About the Reviewers

- **Thomas** has a wealth of experience architecting and delivering cloud-native solutions to global organizations of all sizes. Being recognized as a 'leader who coaches', Thomas is proficient at leading teams as part of larger solution delivery projects or working independently within a virtual team to deliver on specific solution areas.

  He has experience of working in the Microsoft channel and recently in a well-regarded Cyber Risk organization. Tom was responsible for the overall platform architecture of solutions delivered across several SIEM, EDR, NDR, and EASM vendors.

  Tom has earned a mix of vendor certifications from Microsoft, Swimlane, and Armis and holds the ISC2 Certified Cloud Security Professional qualification, demonstrating expertise in multiple domains covering compliance, governance, and cloud security.

- **Fouad** is a seasoned Lead Consultant and Cloud Security Architect with 15 years of professional experience in the digital and software industry at global corporations. Fouad excels in designing and implementing comprehensive cloud solutions across multi-cloud platforms. He has assisted numerous businesses in effectively governing and safeguarding their information, proactively identifying cybersecurity risks, and enabling them to make informed and strategic business decisions. Fouad is CISSP, CISM, CASP+ certified.

- **Dwayne Natwick** is the CEO of Captain Hyperscaler, LLC, a technical cloud and cybersecurity training company. Dwayne was previously the Global Principal Cloud Security Lead at Atos, a multi-cloud GSI. He has been in IT, security design, and architecture for over 30 years. His love for teaching led him to become a Microsoft Certified Trainer (MCT) Regional Lead and a Microsoft Most Valuable Professional (MVP) for Security and Azure.

  Dwayne has a master's degree in Business IT from Walsh College, the CISSP, CGRC, SSCP, and CCSP from ISC2, CRISC from ISACA, and 18 Microsoft certifications, including Identity and Access Administrator, Azure Security Engineer, and Microsoft 365 Security Administrator. Dwayne can be found providing and sharing

information on social media, industry conferences, his blog site, and his YouTube channel.

Originally from Maryland, Dwayne currently resides in Michigan with his wife and three children.

- **Pushkar Nagle** is an InfoSec professional with 13 years of experience, holding professional IT certifications, including CCSP, CISSP, CISM, CEH, and CCNA. Pushkar attained a Licentiate Diploma in Electronics from VJTI, a B.Engg. in Electronics from Mumbai University. Pushkar has held several positions, including penetration tester, vulnerability manager, risk management advisor, and application security consultant. Pushkar has experience in handling large and complex penetration testing projects, providing risk advisory to businesses, and assisting organizations in vulnerability remediation.

  Pushkar has managed 500+ onsite/offsite Web Application pentests, Mobile applications, Infrastructure, Build & Code reviews, and other risk-based security testing projects.

- **Andy Pantelli** is CISSP, CCSP, ACIIS, CCNP Security, CCNP Ent, CCDP, CCNA Cyber Ops, CCNA Security, JNCIP-E, VMware VCP, AWS Cloud Practitioner and Mimecast Secure Email Gateway certified. Previously serving in the Armed Forces, he completed 2 operational tours of duty before settling in the North West of England. He has over 20 years experience in Information Security across the Aviation, Financial, Legal, & Global Media sectors. He is currently a Cyber Security Architect consulting for the UK Central Government.

Acknowledgement

There are a few people I want to thank for their continued and ongoing support, both concerning this book and my cybersecurity career in general.

Firstly, I want to thank my wife for her tireless encouragement and support while writing my first book. I also want to thank my father for his extensive review work throughout the writing process.

Secondly, I want to thank my long-time mentors, "Coach Ron" Woerner and Ralph de Graaf. They have played a vital role in my security journey and have helped me get to where I am now.

Additionally, I want to thank my employer, SimplifyNow, for always supporting my professional growth and allowing me time to dedicate to this book. Together, we are building a safer world.

Lastly, I want to thank the publishing team at BPB for their extensive support, guidance, and assistance in making this book a reality.

Preface

The book will teach you the contrasts and similarities between cloud and on-premises computing. Show you reliable mechanisms to create a secure cloud environment, from the strategic to the operational level. It highlights what security controls help you create a secure cloud from the start and guides you into setting up security processes to keep your cloud secure over time.

The (ISC)2 CCSP is the industry's most sought-after vendor-agnostic cloud security certification. This book prepares you to pass the exam and excel within your business by providing tangible and concrete mechanisms to secure your organization's cloud environment.

The book takes you on a journey throughout all facets of secure cloud computing, from the policies an organization should have to the technical nitty-gritty of securing security groups. The book uses real-life examples, experiences, and tips and tricks from one of the industry's most broadly certified ISC2 professionals.

The book is divided into 24 chapters that cover the domains of the ISC2 CCSP exam. The details are listed below:

Chapter 1: Understanding Cloud Computing Concepts - Cloud computing is different from on-premise computing in many aspects. This chapter highlights definitions related to cloud computing and examines the shared responsibility model between Cloud Service Providers and customers. The chapter reviews cloud computing characteristics and common technologies in the cloud domain and explores the different levels and models for cloud computing

Chapter 2: Concepts and Design Principles of Cloud Security - Security in the cloud relies on foundational concepts and design principles. This chapter explores how cryptography, **Identity and Access Management** (**IAM**), network security, and other concepts form the building blocks of cloud security.

Chapter 3: Evaluating Cloud Service Providers - In a world with a wide variety of Cloud Service Providers, it is challenging to pick a provider that meets your requirements. This chapter helps you pick a CSP by providing methods to evaluate different vendors against your business requirements

Chapter 4: Discover, Classify, and Manage Cloud Data - Storing data in the cloud may sound scary, however, implementing good mechanisms to discover, classify, and manage data in the cloud will offer you unprecedented data security.

Chapter 5: Cloud Storage Architectures and their Security Technologies - Now that you know how data "lives" in the cloud, it is time to explore how different architectures support data types. This chapter explores different architectures for data storage, the threats they face, and what security technologies should be implemented for them.

Chapter 6: Cloud Infrastructure and Components - Cloud infrastructure relies on similar components as on-premise computing. However, how cloud computing is managed is very different from on-premise computing. This chapter explores how cloud infrastructure is set up, used, and managed securely.

Chapter 7: Datacenter Security - You might have heard, "The cloud is just someone else's computer". In this chapter, we explore how data center security is a vital part of cloud computing, regardless of the service model.

Chapter 8: Risk Management in the Cloud - The cloud comes with new and familiar risks, this chapter examines how you can effectively manage and analyze risks within a cloud platform or cloud infrastructure.

Chapter 9: Cloud Security Controls - Understanding and managing risks is extremely important. However, picking the correct controls to (cost) effectively mitigate risk can be extra challenging in the cloud. This chapter covers how you can implement security controls within your cloud environment.

Chapter 10: Business Continuity and Disaster Recovery - While we design for systems and applications to be resilient, things go wrong sometimes. This chapter dives into ensuring your business continuity is ensured, even when things go wrong. The chapter also explains strategies on how to recover from disasters if they do occur.

Chapter 11: Secure Deployment, Awareness, and Training - The cloud offers new perspectives and tools for security, however, developing insecurely is as dangerous in the cloud as it is on-premise. This chapter explores common pitfalls, cloud-based vulnerabilities, and development tactics to ensure the software is developed securely within or outside of the cloud.

Chapter 12: Security Testing and Software Verification - Secure development is essential in creating a secure (cloud) ecosystem. However, while we always aim to develop securely, we must verify that we did so. This chapter explores the role of security testing methods such as static and dynamic code analysis, code review, penetration testing, and functional and non-functional testing. The chapter also sheds light on how APIs can be secured, and vulnerabilities within dependencies or open-source software can be detected.

Chapter 13: Specifics of Cloud Security Architecture - Cloud computing allows us to look at security from a different perspective. This means that we also have to use security

tooling in different places and in different ways. This chapter explores supplemental cloud security components such as web applications firewalls, API gateways, and database activity monitoring. Moreover, the chapter dives into encryption in the cloud, security of virtualization through containers, microservices, and sandboxing

Chapter 14: Identity and Access Management - Broad access is one of the characteristics of the cloud. However, to have broad access and be secure, we must manage identities effectively and securely. This chapter explores how SSO (single sign-on), IdP (identity providers), user federation, secrets management, multi-factor authentication, and **cloud access security brokers** (**CASB**) form the puzzle pieces of secure access in the cloud.

Chapter 15: Infrastructure Security - While **cloud service providers** (**CSPs**) take over a lot of security responsibilities, it is essential to understand the underlying technologies that enable the security functions. This chapter explores how hardware security

models, trusted platform modules, and hypervisor security allow CSPs to create a secure computing environment for their customers.

Chapter 16: Secure Configuration - Security tooling and complex cloud architectures can improve security, however, the configuration powering the tools and systems is what ultimately decides if an ecosystem is secure. This chapter explores the different security policies that must be in place to create a secure environment. It dives into secure network configuration, network security controls, OS Hardening, patch management, Infrastructure as Code, High Availability, Monitoring of performance and hardware, backup, and restore.

Chapter 17: Security Operations - Policies and configuration are essential to create a secure baseline within your environment. However, security processes ensure your environment stays secure over time and adapts to emerging threats. This chapter further expands on security policies, digital forensics, security operations like SOC, SIEM, incident management, and how to communicate with customers, vendors, partners, and others if all our controls prove to be ineffective.

Chapter 18: Legal and Regulatory Requirements in the Cloud - Cloud computing has many benefits, it offers better availability, for example. Some of these characteristics have drawbacks. When talking about legal requirements, the dispersion of data can complicate the scope of regulations your organization must adhere to. This chapter explores various legal requirements and risks associated with computing in the cloud.

Chapter 19: Privacy - Similar to legal requirements, privacy issues can become more complicated in the cloud. It is essential to approach privacy with a well-thought out approach. This chapter zooms in on country-specific legislation, data categories, jurisdictions for privacy, standard privacy requirements, and privacy impact assessments.

Chapter 20: Cloud Auditing and Enterprise Risk Management - The work of developers, system admins, and security engineers is not the only work that changes when switching to cloud computing. Auditors have had to change their approach as well. In an environment with shared responsibilities, auditing can be challenging. This chapter equips you with tactics, tips, and tricks on auditing processes within the cloud, the types of audit reports you might require of a CSP, how you plan audits, and how you can provide auditors with the data they need before they ask for it.

Chapter 21: Contracts and the Cloud - When you decide to use cloud computing within your ecosystem, how you purchase services changes significantly. You will have to ensure the services you purchase live up to your organization's expectations. This chapter explores how you can use service-level agreements, master service agreements, and statements of work to ensure you get the services you need. While vendor, contract, and supply chain management ensure you can prevent issues now and in the future.

Chapter 22: Duties of a CCSP - Passing the CCSP exam allows you to join a select group of cloud security experts. However, being a CCSP or associate of ISC2 also bears Responsibilities. In this chapter, the responsibilities of a CCSP are highlighted based on the ISC2 code of ethics.

Chapter 23: Exam Tips - The exam tips section highlights a breakdown of the exam process and provides tips and tricks to approach the exam most effectively.

Chapter 24: Exam Questions - The exam prep section contains a CCSP practice exam to test your knowledge across the six different domains.

Code Bundle and Coloured Images

Please follow the link to download the
Code Bundle and the ***Coloured Images*** of the book:

https://rebrand.ly/kj3cv76

The code bundle for the book is also hosted on GitHub at
https://github.com/bpbpublications/ISC2-Certified-Cloud-Security-Professional-Exam-Guide
In case there's an update to the code, it will be updated on the existing GitHub repository.

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1
Understanding Cloud Computing Concepts

Introduction

Cloud computing is different from on-premise computing in many ways. This chapter helps you understand the various forms of cloud computing. This chapter will introduce you to the characteristics of cloud computing and standard technologies found in the cloud. It also examines the cloud reference architecture, which outlines responsibilities between **Cloud Service Providers** (**CSPs**), cloud consumers, brokers, and auditors.

Structure

This chapter covers the following topics:

- Cloud computing characteristics
- Public cloud, private cloud, hybrid cloud, community, and multi-cloud
- Cloud operating models (IaaS, PaaS, and SaaS)
- Shared responsibility model
- Cloud reference architecture
- Building block technologies (virtualization, storage, networking, databases, and orchestration)

- Cloud computing characteristics
- The impact of cloud technology

Objectives

In this chapter, you will be able to understand the concepts of cloud computing. You will gain an understanding of the different shapes of cloud computing, the related service models, and the characteristics of cloud computing overall. The chapter will outline how cloud computing environments can integrate with an organization's IT landscape. It will also cover the strengths and weaknesses every cloud computing service model presents and help you determine which model is suitable in what situation. The chapter covers all building block technologies you will see in cloud computing environments while also helping you outline the responsibilities within the cloud.

Essence of cloud computing

Cloud computing. Many people do not know what to expect when they hear this term. However, the essence of cloud computing is simple. Cloud computing is using someone else's computing resources for your computation needs.

Throughout the past decades, we have already been working with forms of cloud computing. Think of web applications offered by third-party providers (**Software as a Service**) or even companies like **Azure** that allow you to rent servers and infrastructure (**Infrastructure as a Service**).

The main difference between current-day cloud computing and the examples above is that companies have branded themselves as **cloud service providers** (**CSPs**). These CSPs have adopted a business model of providing computing services to their customers through on-demand self-service in a scalable fashion. A web hosting company allows you to rent a pre-defined number of servers. But a CSP lets you (automatically) start and create new servers to accommodate more traffic or stop servers or instances when you no longer need them. We call this rapid concept elasticity.

Cloud computing has more benefits than past-day hosting models. One of them is called **measured service**. Measured service means that your usage of the CSPs services is continuously measured, and you only pay for what you use. Combined with rapid elasticity, this offers some attractive benefits.

For example, if your company uses an internal application only during work hours, you can shut down the servers that support the application after work hours. Meaning you would only pay for the hours that the servers were running. If you have a workday from 9 am until 5 pm, you would only pay for 8 hours of operation.

Of course, you could do this in your data center, but you would have to shut down an entire server to save on energy costs. Since you already paid for the servers, turning

them off does not save as much money. If you use virtualization within your data center, shutting down a server might also impact other applications. In short, rapid elasticity can be challenging to achieve in **on-premise computing.**

CSPs use an operating model called **resource pooling** to facilitate rapid elasticity and measured service. Resource pooling means the provider has a pool of computing resources. For example, storage is assigned to a specific customer **on-demand**. On-demand assignment of resources means the following;

In the example above, your company only uses a server during work hours. Once the server shuts down, the available computing resources return to the pool. Similarly, if another CSP customer requires more resources, the compute capacity you just released becomes available to another customer.

EXAM TIP: Resource pooling is a significant risk of cloud computing as it involves sharing hardware resources with other organizations.

The effect of resource pooling is significant to CSPs as it allows them to serve multiple customers without having dedicated hardware for every customer. Limiting the amount of required hardware lets the CSPs control costs. However, it can also bring risks to the table. If customers demand more service than is available, the CSP might not have enough resources to satisfy demand, leading to service outages. On the flip side of this coin, when a CSP overprovisions its resources, and there is little demand, the CSP is incurring high costs for no returns. Many CSPs will offer customers reduced rates if they commit to a minimal pre-determined usage level. Such commitments allow the CSP to determine better how much hardware should be available, preventing the resources from being over - or under-leveraged.

The last characteristic of cloud computing is called **broad network access**. Broad network access means cloud computing resources are available to customers online. Most CSPs (like **AWS**, **Microsoft Azure**, and **GCP**) offers an online portal that allows you to log in and provision your resources on demand over the internet. Contrary to on-premise computing, where the need for new resources requires the purchase of new servers and access to the physical site of the devices. Broad network access makes cloud computing easy.

To summarize, NIST defines the five characteristics of cloud computing: on-demand self-service, broad network access, rapid elasticity, measured service, and resource pooling. These characteristics will be the red line throughout this book, presenting many significant strengths and specific security challenges.

Cloud comes in many shapes

Cloud computing is applicable in different ways. An organization might use cloud computing for all or some of its workloads. A computing cloud environment is creatable at different scopes as well. Some clouds serve a single company, while others might help

a whole community of companies. Regardless of the shape of cloud computing used, every model has its benefits and drawbacks. Lets us explore the different forms of cloud computing that exist.

Public cloud is probably one of the most well-known shapes of cloud computing. In a public cloud, a CSP provides cloud computing services to virtually anyone wanting to purchase them. The CSP wants to make it easy for customers to consume their services. Because a public cloud provides services to a broad audience, they usually are very good at self-service provisioning. However, a public cloud also means many customers share the available resources. When you share resources with other organizations, you must realize that this creates security risks.

An attacker on a completely unrelated company could cause service outages (or worse) to your organization. For example, if another customer is hosting a virtual machine on the same server your virtual machine is running, and an attacker can break out of the virtual machine of the other company, they can potentially disrupt the availability of the underlying server. Of course, cloud providers take measures to prevent such events from occurring, and we will examine those measures throughout the book.

Private cloud is a form of cloud computing where the hardware (and infrastructure) used is exclusive to a single customer, or the company itself owns and manages the hardware. A private cloud is generally more secure but almost always more costly. If the organization operates the private cloud, it also involves more effort and knowledge of secure design and operations. Many CSPs provide private cloud services to the customer by allowing them to reserve hardware for their organization only. Other large parties, like governmental agencies, even build their cloud computing environments in their data centers. When a company or governmental agency creates its cloud, they act as the CSP and the consumer. The consumer can then still benefit from the characteristics of cloud computing without having to share underlying infrastructure with other organizations.

Hybrid Cloud is a form of cloud computing where private and public clouds are combined. A hybrid cloud allows an organization to pick and choose where they want to process specific workloads. Determining where you process a workload will enable you to separate sensitive workloads. You might not want to process in a public cloud from everyday computing that does not require dedicated infrastructure. Public and private cloud environments are often connected using dedicated connections such as VPNs or even leased lines. The following table shows examples of the composition of different cloud shapes:

Public cloud	Private cloud	Hybrid cloud	Multi cloud
Microsoft Azure	on-premise data center	on-premise data center	Microsoft Azure
OR		AND	AND

Public cloud	Private cloud	Hybrid cloud	Multi cloud
Amazon Web Services (AWS)		Amazon Web Services (AWS)	Amazon Web Services (AWS)
OR			AND
Google Cloud Platform (GCP)			Google Cloud Platform (GCP)

***Table 1.1**: Examples of public, private, hybrid, and multi-cloud setups*

Community cloud is a form of cloud computing where multiple organizations share the same computing environment. Community clouds are common for organizations that collaborate. For example, universities that perform research projects can benefit from using a shared cloud environment to process and share research results. Sharing a computing environment with other organizations can pose security risks, as every organization must ensure its internal security practices are in line.

For example, if university A uses usernames and passwords to authenticate and University B uses **Multi-Factor Authentication** (**MFA**). Attackers would be far more likely to gain access to the environment through a compromised university A user. Therefore, it is essential to create a standard set of controls that establishes a security baseline of how the community cloud should be secured, configured, and operated between all organizations.

Multi-cloud is the last form of cloud computing to cover. A multi-cloud environment is an environment that exists out of multiple cloud environments. For example, a multi-cloud environment might have a **Microsoft Azure environment** and an **Amazon Web Services** (**AWS**) **environment**. Separating your computation needs over multiple clouds allows you to leverage specific tools that a CSP has to offer. Those tools might work better at one CSP than the other, or costs might be lower at one CSP than the other. However, many organizations also choose a multi-cloud environment to fight the risk of vendor lock-in. Vendor lock-ins are not specific to cloud computing and mean that you establish a dependency on a single vendor that might force you to keep doing business with them as your operations are highly dependent on the vendor.

In some cases, this dependency on a vendor can be dangerous. For example, a vendor promises to perform security patches daily per their **service level agreement** (**SLA**). But it turns out your vendor does not do this. Your organization confronts the vendor, but the vendor refuses to fix the issue. Your organization might choose to pull out of the contract, but if all your online services are hosted at this vendor, pulling out might mean you have to shut down your services. Shutting down the services for a prolonged period can significantly damage an organization. Multi-cloud attempts to solve this, allowing you to build the same online services at two vendors. If you properly sync data between the environments, you can shut down the environment at the vendor you no longer want to work with and continue with the other vendor. Remember that not every multi-cloud