4th Edition

Certified Cloud Security Professional

An (ISC)² Certification

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

Aaron Kraus

SYBEX
A Wiley Brand

The Official (ISC)^{2}® CCSP® CBK® Reference

Fourth Edition

CCSP®: Certified Cloud Security Professional

An (ISC)²® Certification

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

Fourth Edition

Aaron Kraus

SYBEX®
A Wiley Brand

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

ISBN: 978-1-119-90901-9
ISBN: 978-1-119-90902-6 (ebk.)
ISBN: 978-1-119-90903-3 (ebk.)

Library of Congress Control Number: 2022941286

Cover design: Wiley and (ISC)²

Acknowledgments

First and foremost, my deepest appreciation goes to my family, mentors, and colleagues. The support of my family during the long hours required to research, write, and review this book made it possible. Mentors and colleagues who have educated and guided me made it possible to produce this reference, and the excellent resources they have created are linked throughout the book for more information on a wide variety of topics.

I would also like to express appreciation to (ISC)² for providing the CCSP certification, certification preparation materials, and reference guides for many security topics. As the world continues the shift to cloud computing, it is essential for security practitioners to have validated real-world skills to properly secure these new computing resources.

The excellent team at John Wiley & Sons is a continuing source of support, including associate publisher Jim Minatel, project editor John Sleeva, and content refinement specialist Archana Pragash. Many thanks to them for entrusting me with the task of updating this reference guide and for their ongoing help to make it the best possible. Special thanks to my technical editor Gareth Marchant, whose knowledge and insight elevated every domain.

Above all, thank you to the readers. Whether you are preparing for your CCSP exam or brushing up on a crucial aspect of cloud security, it is your hard work securing cloud computing environments that makes the world a safer place.

About the Author

Aaron Kraus, CCSP, CISSP, is an information security executive with deep experience in security risk management, auditing, and teaching information security topics. He has worked in security and compliance roles across industries including U.S. federal government civilian agencies, financial services, and technology startups, and he is currently a security director for a property technology startup. His experience includes creating alignment between security teams and the organizations they support, by evaluating the unique threat landscape facing each organization and the unique objectives each organization is pursuing to deliver a balanced, risk-based security control program. As a consultant to a financial services firm, he designed, executed, and matured the third-party vendor audit programs to provide oversight of key compliance initiatives, and he led global audit teams to perform reviews covering physical security, logical security, and regulatory compliance. Aaron is a course author, instructor, and cybersecurity curriculum dean with more than 14 years of experience at Learning Tree International, and he most recently taught the Official (ISC)² CISSP CBK Review Seminar. He has served as a technical editor for numerous Wiley publications, including CISSP and CCSP study guides and practice tests, and is coauthor of *The Official (ISC)² CISSP CBK Reference* as well as coauthor of the previous edition of *The Official (ISC)² CCSP CBK Reference*.

About the Technical Editor

Gareth Marchant started his professional career as an electrical engineer and has worked in information technology for over 20 years. He has held systems engineering and senior leadership roles in both private and public sector organizations. The central theme throughout his career has been systems architecture and design, covering a broad range of technical services but always focused on resiliency. Gareth currently lives in Nashville, TN, but has recovered IT operations in Florida following tornado strikes and many hurricanes.

Gareth is an (ISC)^2 and EC-Council certified instructor and currently holds CISSP, CEH, ECIH, SSCP, GMON, CASP+, Security+, CySA+, Network+, Cybersec First Responder, Cyber Secure Coder, and other certifications, as well as a master's degree in computer information systems. In addition to cybersecurity certification prep, he also teaches information systems and cybersecurity courses as an adjunct instructor and is the author of the *Official CompTIA CASP+ Self-Paced Study Guide*.

Contents at a Glance

Contents

Foreword to the Fourth Edition

These are exciting times for the cybersecurity profession, and we are so glad that you are a part of it. Once recognized as a CCSP®, you will have a cloud security certification that will help you advance your career by demonstrating your expertise in securing critical assets in the cloud.

Cloud security is one of the most in-demand cybersecurity skillsets today. In fact, the opportunity has never been greater for dedicated professionals to carve out a meaningful career and make a difference in their organizations. Earning the CCSP® certification makes you a forerunner in the cybersecurity community, proving that you have the advanced skills and knowledge to design, manage, and secure data, applications, and infrastructure in the cloud.

Whether you are picking up this book in preparation to sit for the exam or you are an existing CCSP® using this as a reference, you'll find *Official (ISC)² CCSP CBK Reference* a valuable resource as you continue to learn about today's cloud security principles and practices.

We wish you all the best in your CCSP® journey. From the very beginning through the advancements and discoveries that you are sure to find along the way, (ISC)² will be by your side, always advocating for you, as we work together to create a safe and secure cyber world.

Sincerely,

Clar Rosso

Clar Rosso

CEO, (ISC)²

Introduction

The Certified Cloud Security Professional (CCSP) denotes a professional with demonstrated ability across important aspects of architecture, data security, and risk management in cloud computing. The exam covers knowledge and skills across six domains of practice related to cloud security, codified in the (ISC)^2 CCSP Common Body of Knowledge (CBK).

- Domain 1: Cloud Concepts, Architecture, and Design
- Domain 2: Cloud Data Security
- Domain 3: Cloud Platform and Infrastructure Security
- Domain 4: Cloud Application Security
- Domain 5: Cloud Security Operations
- Domain 6: Legal, Risk, and Compliance

Passing the exam is one condition of certification, and to qualify for the certification, a professional must have five years of experience in information technology, of which three years must be in a security-specific capacity and at least one year dedicated to one or more of the six CCSP domains.

Professionals take many paths into information security, and there are variations in acceptable practices across different industries and regions. The CCSP CBK represents a baseline standard of security knowledge relevant to cloud security and management, though the rapid pace of change in cloud computing means a professional must continuously maintain their knowledge to stay current. As you read this guide, consider not only the scenarios or circumstances presented to highlight the CBK topics, but also connect it to common practices and norms in your organization, region, and culture. Once you achieve CCSP certification, you will be asked to maintain your knowledge with continuing education, so keep topics of interest in mind for further study once you have passed the exam.

Domain 1: Cloud Concepts, Architecture, and Design

Understanding cloud computing begins with the building blocks of cloud services, which the Cloud Concepts, Architecture, and Design domain introduces. This includes two vital participants: cloud service providers and cloud consumers, as well as reference architectures used to deliver cloud services like infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). There are business benefits inherent in these IT resource paradigms, like shifting spending from capital expenditure (CapEx) to operating expenditure (OpEx). This changes the way organizations budget and pay for the IT resources needed to run their business, so it is not uncommon to see financial leaders driving adoption of cloud services. New IT service models bring with them new forms of information security risks, however, which must be assessed and weighed so the organization achieves an optimal

balance of cost (in the form of risk) with benefits (in the form of reduced IT spending). This will drive decisions on which cloud deployment model to adopt, like public or private cloud, as well as key internal governance initiatives when migrating to and managing cloud computing.

Domain 2: Cloud Data Security

Information security is fundamentally concerned with preserving the confidentiality, integrity, and availability of data. Although cloud computing upends many legacy IT models and practices, security risks to information systems remain. The Cloud Data Security domain introduces new concepts like the cloud data lifecycle, as well as cloud-specific considerations like data dispersion and loss of physical control over storage media that requires unique approaches to data disposal. Cloud security practitioners must understand how to implement controls for audit and accountability of data stored or processed in the cloud, as well as crucial oversight tasks like data discovery to create an inventory. This domain introduces proactive safeguards intended to manage sensitive data stored in the cloud, like masking, tokenization, data loss prevention (DLP), and classification of data. Cloud-specific considerations and adaptations of traditional controls are a primary concern, since cloud services remove security capabilities like physical destruction of disk drives. Cloud computing also introduces new capabilities like instantaneous global data replication, which can reduce availability risks.

Domain 3: Cloud Platform and Infrastructure Security

There are two perspectives treated in the Cloud Platform and Infrastructure Security domain. Cloud providers require skilled security practitioners to design, deploy, and maintain both physically and logically secure environments. This includes buildings, facilities, and utilities needed to provide the cloud service offering, as well as configuration and management of software systems like hypervisors, storage area networks (SANs), and software-defined networking (SDN) infrastructure. A key concern is the security of data stored by the cloud consumers, particularly the proper isolation of tenant data to avoid leakage between cloud tenants. From the perspective of the cloud consumer, traditional security controls will require adaptation for cloud environments, such as the use of virtualized hardware security modules (HSM) to generate and manage cryptographic keys, and additional layers of encryption required to reduce the risk associated with giving up physical control of storage media. Audit mechanisms like log collection are generally available in cloud environments, but abilities like packet capture and analysis may not be available due to multitenant data concerns. Disaster recovery and business continuity planning are also presented in this domain; while the inherent high availability of many cloud services is beneficial for organizations, proper configuration to take advantage of these features is required.

Domain 4: Cloud Application Security

Security practitioners working in cloud computing environments face the challenge of more rapid deployment, coupled with the relative ease with which more users can develop sophisticated cloud applications. Again, these are advantages to the business at the possible expense of security, so the Cloud Application Security domain presents key requirements for recognizing the benefits offered by cloud applications without introducing unacceptable risks. These begin with a focus on the importance of fostering awareness throughout the organization of common cloud security basics. Specific training for cloud app developers on vulnerabilities, pitfalls, and strategies to avoid them is also presented. Modifications to the software development life cycle (SDLC) are discussed, which help accommodate changes introduced by cloud-specific risks. These include system architecture concerns to avoid vendor lock-in and threat modeling specific to the broadly accessible nature of cloud platforms. Since many cloud computing services are delivered by third parties, this domain introduces assurance, validation, and testing methods tailored to address the lack of direct control over acquired IT services and applications. It also introduces common application security controls and specifics of their implementation for cloud environments, like web application firewalls (WAF), sandboxing, and Extensible Markup Language (XML) gateways. Many cloud services rely heavily on functionality offered via application programming interfaces (APIs), and key points regarding how data is exchanged, processed, and protected by APIs are presented in this domain.

Domain 5: Cloud Security Operations

The Cloud Security Operations domain is a companion to many of the concepts introduced in the Cloud Platform and Infrastructure Security domain. It deals with issues of implementing, building, operating, and managing the physical and logical infrastructure needed for a cloud environment. There is a heavy focus on the cloud service provider's perspective, so concepts in this domain may be unfamiliar to some security practitioners who have only worked to secure cloud services as a consumer. The concepts are largely similar to legacy or on-premises security, such as the secure configuration of BIOS and use of Trusted Platform Module (TPM) for hardware security, deployment of virtualization management tools, and configuring remote maintenance capabilities to allow remote administrative tasks. Considerations unique to cloud environments include the additional rigor required in the configuration of isolation features, which prevent data access across tenants, as well as the much larger demands of managing capacity, availability, and monitoring of vast, multicountry data centers. Traditional security operations (SecOps) are also of critical concern for security practitioners in a cloud environment, such as handling vulnerability and patch management programs, network access and security controls, and configuration and change management programs. Additional SecOps activities covered in this domain include supporting incident response and digital forensics when security incidents occur, as well as traditional security

operations center (SOC) oversight and monitoring functions for network security, log capture and analysis, and service incident management. These tasks are also covered from the cloud consumer's perspective, as many cloud services and security tools provide log data that must be analyzed to support policy enforcement and incident detection.

Domain 6: Legal, Risk, and Compliance

Legal and regulatory requirements are a significant driver of the work many information security professionals perform, and cloud computing adds increased complexity due to its inherently global nature. The Legal, Risk, and Compliance domain details the conflicting international laws and regulations that organizations will encounter when using cloud services. These present financial risks, additional compliance obligations and risk, and technical challenges like verifying that cloud applications and services are configured in accordance with compliance requirements. Privacy legislation is a particularly important driver of many cloud security concerns; as many countries and localities introduce strict requirements to safeguard privacy data, organizations using the cloud must weigh financial benefits of a cloud migration against potential fines if they violate these laws. New challenges are also emerging around jurisdiction over multinational cloud services: how do you determine jurisdiction for a U.S.-based company operating a cloud data center in Kenya processing data belonging to a Swiss citizen? Three different laws potentially overlap in this scenario. Processes for audits, assurance, and reporting are also covered, as security practitioners must understand and be able to implement both internal oversight mechanisms like gap analysis and audit planning, while also selecting and supporting external auditors for standards like Service Organization Control (SOC) audit reports. Since cloud service providers are third parties not directly under the control of the organization, vendor risk management practices like contract design and service level agreements (SLAs) are often required tools for security risk management.

Chapter 1

Cloud Concepts, Architecture, and Design

Domain 1 establishes the foundation of knowledge required to adequately secure cloud environments, including an overview of key architectural concepts and security principles applied to cloud environments. This information is fundamental for all other topics in cloud computing. A set of common definitions, architectural standards, and design patterns will put everyone on the same level when discussing these ideas and using the cloud effectively and efficiently.

Understand Cloud Computing Concepts

The first task is to define common concepts. In the following sections, we will provide common definitions for cloud computing terms and will discuss the various participants in the cloud computing ecosystem. We will also discuss the characteristics of cloud computing, answering the question "What is cloud computing?" We will also examine the technologies that make cloud computing possible.

Cloud Computing Definitions

Cloud computing is a quickly evolving practice, with new concepts and paradigms of computing being introduced quickly. Cloud computing itself represented a major shift from traditional on-premises infrastructure, data centers, and colocation facilities, and to apply security to these new environments it is essential to have a firm understanding of core concepts.

Cloud Computing

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145 provides a widely accepted definition of cloud computing: "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort or service provider interaction." The document formalizes definitions of cloud computing and services, including the five essential characteristics that define a cloud service, cloud service categories, and deployment models. These are discussed in more detail later in this chapter.

Cloud computing expands earlier concepts of distributed computing or parallel computing, even when done over a network, in a number of critical ways. It is a philosophy that creates access to computing resources in a simple, self-driven way. Although an organization or individual may negotiate a contract, rates, and service levels from a cloud provider, once access is granted a true cloud computing environment typically does not require involvement by the cloud service provider (CSP).

Cloud computing requires a network in order to provide broad access to infrastructure, development tools, and software solutions. It requires some form of self-service to allow users to reserve and access these resources at times and in ways that are convenient to the user.

The provisioning of resources needs to be automated so that human involvement is limited. Any user should be able to access their account and procure additional resources or reduce current resource levels by themself, without the need for manual work by the CSP staff.

An example is Dropbox, a cloud-based file storage system. An individual creates an account, chooses the level of service they want or need, and provides payment information. Once this is done, the service and storage are immediately available. A company might negotiate contract rates more favorable than are available to the average consumer, but once the contract is in place, the company's employees can access this resource without the need for any additional provisioning by Dropbox staff.

A final important concept in cloud computing deals with the financial accounting for cloud services. While this is typically outside the role of the security practitioner, it is a key driver for many organizations adopting cloud computing and is helpful to understand. Purchasing servers and building data centers to house them are known as capital expenditures (CapEx), while services like cloud computing are known as operating expenditures (OpEx). In most places OpEx spending is preferable due to more favorable tax treatment; whatever an organization spends in OpEx reduces taxable income, thereby reducing the organization's tax bill.

Service and Deployment Models

There are three *service models* and four *deployment models* in which cloud services can be provisioned. These are discussed in detail later in this chapter, but a basic understanding is essential to begin exploring other cloud concepts.

The three service models are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). The key differences between these models include the level of control the consumer has over the cloud service as well as the level of effort required to use the service.

There are four deployment models for cloud services: public, private, community, and hybrid clouds. These define who owns and controls the underlying infrastructure of a cloud service and who can access a specific cloud service. Additionally, organizations may adopt a multi-cloud deployment strategy, combining two or more of these deployment models across their technology stack.

These concepts will be discussed further in the "Cloud Service Categories" and "Cloud Deployment Models" sections later in this chapter.

Cloud Computing Roles and Responsibilities

There are a number of roles in cloud computing, and understanding each role allows clearer understanding of each of the cloud service models, deployment models, security responsibilities, and other aspects of cloud computing.

Cloud Service Customer

The cloud service customer (CSC) is the company or person purchasing the cloud service, or in the case of an internal customer, the employee using the cloud service. For example, a SaaS CSC would be any individual or organization that subscribes to a cloud-based email service. A PaaS CSC would be an individual or organization subscribing to a PaaS resource. A PaaS resource could be a development platform. With an IaaS solution, the customer is a system administrator who needs infrastructure to support their enterprise. The CSC consumes the services provided by the cloud service provider.

Cloud Service Provider

The CSP is the company or other entity offering cloud services. CSPs may be public companies providing cloud services to any customer but can also be an internal IT department that provisions cloud platforms to other units of the organization. A CSP may offer SaaS, PaaS, or IaaS services in any combination. For example, major CSPs such as AWS, Microsoft Azure, and Google Cloud offer both PaaS and IaaS services. Major SaaS CSPs include companies like Salesforce and Dropbox, as well as Microsoft 365 and Google Workspace, which are SaaS offerings built on top of the same cloud components that make up Azure and Google Cloud.

As the cloud environment becomes more complicated, with hybrid clouds and community clouds that federate across multiple cloud environments, the responsibility for security becomes ever more complex. As the customer owns their data and processes, they have a responsibility to review the security policies and procedures of any and all CSPs in use at their organization, and the federated responsibilities that may exist between multiple CSPs and data centers.

Cloud Service Partner

A cloud service partner is a third-party offering a variety of cloud-based services (infrastructure, storage and application services, and platform services) using the associated CSP. An AWS cloud service partner uses AWS to provide their services. The cloud service partner can provide customized interfaces, load balancing, and a variety of services. It may be an easier entrance to cloud computing, as an existing vendor may already be a cloud service partner. The partner has experience with the underlying CSP and can introduce a customer to the cloud more easily.

The cloud partner network is also a way to extend the reach of a CSP. The cloud service partner will brand its association with the CSP. Some partners align with multiple CSPs, giving the customer a great deal of flexibility. Partners can extend the value of cloud services by selling additional services, support, management, and consulting to organizations that lack these skills or capabilities.

Cloud Service Broker

A cloud service broker is similar to a broker in any industry. Companies use a broker to find solutions to their cloud computing needs. The broker will package services in a manner that

benefits the customer. This may involve the services of multiple CSPs. A broker is a value-add service and can be an easy way for a company to begin a move into the cloud. A broker adds value through aggregation of services from multiple parties, integration of services with a company's existing infrastructure, and customization of services that a CSP cannot or will not make. They may also be able to offer discounts due to volume purchasing of cloud services, which is beneficial to smaller organizations that lack the bargaining power of a high-volume purchaser.

Just as with any vendor, it is crucial to vet the capabilities and reputation of a CSB before engaging their services. Each serves a specific market, utilizing different cloud technologies. It is important that the CSBs selected are a good fit for the customer organization and its cloud strategy. While this is typically an operational concern rather than a security one, inadequate capabilities in the cloud solution can give rise to security problems if needed security controls cannot be implemented.

Regulator

Cloud computing itself is not heavily regulated, similar to most IT environments, which are merely tools. The use of those tools, specifically the processing of data, is regulated. Examples of regulatory frameworks that govern cloud data processing include the European Union General Data Protection Regulation (EU GDRP), the Graham-Leach-Bliley Act (GLBA), and the Personal Information Protection and Electronic Documents Act (PIPEDA), which are privacy laws in Europe, the United States, and Canada, respectively. While none explicitly identify cloud computing, they do require organizations that collect, process, or store data to properly safeguard it. Cloud customers must be aware of any regulations that affect their data or business processes and choose or configure CSP resources that meet those regulatory requirements.

Common regulatory issues that impact cloud usage include security of data at rest and in transit. When looking at data in a cloud environment, the broad network accessibility characteristic usually requires the use of the Internet to interact with systems, so these regulations demand adequate encryption to protect the data as it moves into and out of the cloud. Similarly, the shared multitenant nature of cloud services and involvement of third-party administrators working for the CSP demand proper controls for the data at rest; encryption is a common control that can mitigate the risk of unauthorized disclosure so long as keys are properly managed.

Regulatory bodies have published guidance for organizations utilizing cloud computing services to handle sensitive data, and CSPs share responsibility for providing service offerings that are compliant with their customers' regulatory requirements. For example, the major CSPs offer configurations of many services that are compliant with various regulations, though there may be additional costs associated with these specialized offerings. Ultimately it is the responsibility of the consumer to identify all requirements associated with their data and choose, architect, and maintain cloud solutions in line with those requirements.

Examples of regulator guidance on cloud computing include the following:

- UK Information Commissioner's Office, *Guidance on the use of cloud computing*: `ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf`

- Irish Data Protection Commission, *Guidance for Organisations Engaging Cloud Service Providers*: dataprotection.ie/sites/default/files/uploads/2019-10/Guidance%20for%20Engaging%20Cloud%20Service%20Providers_Oct19.pdf
- U.S. Department of Health and Human Services Guidance on HIPAA & Cloud Computing: hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html

Shared Responsibility Model

Depending on the service provided (SaaS, PaaS, or IaaS), the responsibilities of the CSP vary considerably. In all cases, security in the cloud is a shared responsibility between the CSP and the customer. This shared responsibility is a continuum, with the customer taking a larger security role in an IaaS service model and the CSP taking a larger role in the security of a SaaS service model. The responsibilities of a PaaS fall somewhere in between. But even when a CSP has most of the responsibility in a SaaS solution, the customer is ultimately responsible for the data and processes they put into the cloud.

The major CSPs publish their variations of a *shared responsibility model* detailing the assignment of various aspects of security to the CSP, the CSC, or both. In most cases, the CSP is solely responsible for operational concerns such as environmental controls within the data center, as well as security concerns such as physical access controls. Customers using the cloud service are responsible for implementing data security controls, such as encryption, that are appropriate to the type of data they are storing and processing in the cloud. Some areas require action by both the provider and customer, so it is crucial for a CCSP to understand which cloud service models are in use by the organization and which areas of security must be addressed by each party. The generic model in Table 1.1 identifies key areas of responsibility and ownership in various cloud service models.

TABLE 1.1 Cloud Shared Responsibility Model

Responsibility	IAAS	PAAS	SAAS
Data classification	C	C	C
Identity and access management	C	C/P	C/P
Application security	C	C/P	C/P
Network security	C/P	P	P
Host infrastructure	C/P	P	P
Physical security	P	P	P

C = Customer, P = Provider

A variety of CSP-specific documentation exists to define shared responsibility in each CSP's offerings, and a CCSP should be familiar with the particulars of the provider their organization is utilizing. The following is a brief description of the shared responsibility model for several major CSPs and links to further resources:

- **Amazon Web Services (AWS)**: Amazon identifies key differences for responsibility "in" the cloud versus security "of" the cloud. Customers are responsible for data and configuration in their cloud apps and architecture, while Amazon is responsible for shared elements of the cloud infrastructure including hardware, virtualization software, environmental controls, and physical security.

  More information can be found here: `aws.amazon.com/compliance/shared-responsibility-model`.

- **Microsoft Azure**: Microsoft makes key distinctions by the service model and specific areas such as information and data and OS configuration. Customers always retain responsibility for managing their users, devices, and data security, while Microsoft is exclusively responsible for physical security. Some areas vary by service model, such as OS configuration, which is a customer responsibility in IaaS but a Microsoft responsibility in SaaS.

  More information can be found here: `docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility`.

- **Google Cloud Platform (GCP)**: Google takes a different approach with a variety of shared responsibility documentation specific to different compliance frameworks such as ISO 27001, SOC 2, and PCI DSS. The same general rules apply, however: customer data security is always the customer's responsibility, physical security is always Google's responsibility, and some items are shared depending on what service offerings are utilized.

  More information can be found here: `cloud.google.com/security`.

Key Cloud Computing Characteristics

The NIST SP 800-145 definition of cloud computing describes certain characteristics that must be present for an IT service to be considered a cloud service. Not every third-party solution is a cloud solution. Understanding the key characteristics of cloud computing will allow you to distinguish between cloud solutions and noncloud solutions. This is important as these characteristics result in certain security challenges that may not be shared by noncloud solutions.

On-Demand Self-Service

The NIST definition of cloud computing identifies an on-demand service as one "that can be rapidly provisioned and released with minimal management effort or service provider interaction." This means the user must be able to provision these services simply and easily when they are needed. If you need a Dropbox account, you simply set up an account and

pay for the amount of storage you want, and you have that storage capacity immediately. If you already have an account, you can expand the space you need by simply paying for more space. The access to storage space is on demand; neither creating an account nor expanding the amount of storage available requires the involvement of people from the CSP. This capability is automated and provided via a dashboard or other simple interface.

On-demand self-service offers advantages of speed and flexibility compared to traditional IT services that required lengthy provisioning processes. However, this ease of use can facilitate the poor practice known as *shadow IT*. Any individual, team, or department can bypass company policies and procedures that handle the provisioning and control of IT services. A team that wants to collaborate can choose and provision OneDrive, Dropbox, SharePoint, or another service to facilitate collaboration. This can lead to sensitive data being stored in locations that do not adhere to required corporate controls and places the data in locations the larger business is unaware of and cannot adequately protect.

In the past, provisioning IT resources involved significant spending, but the pricing of cloud services may fall below spending thresholds that require reviews and approvals. Large projects typically require some reviews and approvals from departments such as finance, accounting, IT, security, or vendor management. Setting up a cloud service is typically much cheaper and can be done using a credit card, meaning the new IT service circumvents processes designed to evaluate and mitigate security risks.

If this behavior is allowed to proliferate, the organization can lose control of its sensitive data and processes. For example, the actuary department at an insurance company may decide to create a file-sharing account on one of several available services. As information security was not involved, company policies, procedures, risk management, and controls programs are not followed. As this is not monitored by the security operations center (SOC), a data breach may go unnoticed, and the data that gives the company a competitive advantage could be stolen, altered, or deleted. Counterintuitively, shadow IT can also lead to increased spending. If all departments set up and maintain their own cloud environments, the organization loses the ability to negotiate lower rates in exchange for volume purchasing, and different groups may even pay for the same services, potentially doubling costs.

Broad Network Access

Cloud services assume the presence of a network. For public and community clouds, this is the Internet. For a private cloud, it could be the corporate network—generally an IP-based network—and possibly the Internet and a secure remote access method such as a VPN. In either case, cloud services are not local solutions stored on your individual computer. They are solutions that require the use of a network to access services hosted in the cloud. Without broad and ubiquitous network access, the cloud becomes inaccessible and is no longer useful.

Not all protocols and services on IP-based networks are secure. Part of the strategy to implementing a secure cloud solution is to choose secure protocols and services. For example, Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP) should not be used to move data to and from cloud services as they send unencrypted data. HTTP Secure (HTTPS), Secure FTP (SFTP), and other encryption-based transmission should be used so that data in motion may be intercepted but not read.

If you are able to access the cloud service and obtain access to your data anywhere in the world, so can others. The requirement for identification and authentication becomes more important in this public-facing environment. The security of accessing your cloud services over the Internet can be improved in a number of ways including improved passwords, multifactor authentication (MFA), virtual private networks (VPNs), etc. The increased security needs of a system available over the network where security is shared between the CSP and customer makes these additional steps more important. For clouds that require remote access, traditional security models that assume a secure perimeter are no longer applicable. This drives new requirements for network security such as zero trust architecture, which is discussed later in this chapter.

Multitenancy

One way to get the improved efficiencies of cloud computing is through the sharing of infrastructure. CSPs provide a virtual set of resources including memory, computing power, and storage space, which customers share. This is known as a multitenant model, similar to an apartment building where tenants share resources and services but have their own dedicated space. Virtualization enables the appearance of single tenancy in a multitenancy situation. Ideally, each tenant's data remains private and secure in the same way that your belongings (data) in an apartment building remain secure and isolated from the belongings (data) of your neighbor. However, incorrect access settings and software flaws in virtualization software may be exploitable to grant unauthorized access.

In a multitenant model it is the responsibility of each tenant to exercise care to maintain the integrity and confidentiality of their own data. If your apartment door is left unsecured, any other tenant in the building could easily enter and steal your belongings. It is also necessary to consider the availability of the data, as the actions of the CSP or another tenant could make your data inaccessible for a time due to no fault of your own. A software upgrade that causes system outages could impact other users of shared infrastructure, just as a fire in one apartment could cause damage to surrounding apartments. A multitenant environment increases the importance of disaster recovery (DR) and business continuity (BC) planning; luckily, other aspects of cloud services make planning high-availability (HA) infrastructure easier and cheaper.

Rapid Elasticity and Scalability

In a traditional computing model, a company needs to plan and buy for anticipated infrastructure needs. If they estimate poorly, they will either have too little capacity, leading to loss of availability, or have excess capacity that represents wasted money. In a cloud solution, elastic infrastructure allows the service to grow or shrink as needed to support the customer's demand. If there is a peak in usage or resource needs, the service grows, or scales, to meet the demand. When usage falls back to normal levels, the resources are released. This supports a pay-as-you-go model, where a customer pays only for the resources they actually consumed rather than excess capacity for potential future needs.

For the CSP, this presents a challenge. The CSP must have the excess capacity to serve all their customers without having to incur the cost of the total possible resource usage. They

must, in effect, estimate how much excess capacity they need to serve all of their customers. If they estimate poorly, the customer will suffer, and the CSP's customer base could decrease.

There is a cost to maintaining this excess capacity. The cost must be built into the cost model. In this way, all customers share in the cost of the CSP, maintaining some level of excess capacity. However, some cloud customers can achieve cost savings by sharing excess capacity only when they need it. For example, an online retail store is likely to need excess capacity during major holidays, while a tax preparer needs it at a different time. Both organizations can access the resources as demand peaks, without having to pay for the full set of resources during nonpeak seasons.

In the banking world, a bank must keep cash reserves of a certain percentage so that it can meet the withdrawal needs of its customers. But if every customer wanted all of their money at the same time, the bank would run out of cash on hand. In the same way, if every customer's potential peak usage occurred at the same time, the CSP would run out of resources, leading to a loss of availability and unhappy customers.

The customer must also take care in setting internal limits on resource use. Proper architectural decisions as well as process and procedure are required to ensure that resources that are no longer needed are deprovisioned. Otherwise, the customer continues to pay for resources that are not serving any purpose. Some cloud service offerings provide automated scale-up and scale-down capabilities, but it is possible to design cloud architecture that mimics traditional servers in a data center with no automated scaling.

Resource Pooling

In many ways, this is the core of cloud computing. Multiple customers share a set of resources including compute power, memory, storage, application services, etc. They do not each have to buy the infrastructure necessary to provide their IT needs. Instead, they share these resources with each other through the orchestration of the CSP. Everyone pays for what they need and use. Pooling these resources enables the other characteristics of cloud computing: self-service is possible because adding a new virtual server doesn't require a physical server to be installed and set up, and automating this based on demand is what enables elasticity.

This resource pooling presents some challenges for the cybersecurity professional, including issues of multitenancy as discussed earlier. A competitor or a rival can be sharing the same physical hardware. If the system, especially the hypervisor, is compromised, sensitive data could be exposed.

Resource pooling also implies that resources are allocated and deallocated as needed. The inability to ensure data erasure can mean that remnants of sensitive files could exist on storage allocated to another user. This increases the importance of data encryption and key management.

Measured Service

Metering service usage allows a CSP to charge for the resources used. In a private cloud, this can allow an organization to charge each department based on their usage of the cloud. For

a public cloud, it allows each customer to pay for the resources used or consumed. With a measured service, everyone pays their share of the costs.

Measured service provides two key benefits. It is the foundation of shifting IT spending from CapEx to OpEx, and it provides additional visibility and transparency into actual IT needs. A CSP provides metrics on the services consumed, including network bandwidth, storage space, and computing power. This discrete measurement of services consumed is in contrast to estimating how much of a server's capacity is actually used and is beneficial for capacity planning.

Building Block Technologies

These technologies are the elements that make cloud computing possible. Without virtualization, there would be no resource pooling, while advances in networking allow for ubiquitous access. Improvements in storage and databases allow remote access to virtual storage in a shared resource pool, and orchestration puts all the pieces together and allows organizations to utilize the various cloud computing services. The combination of these technologies allows better resource utilization and improves the cost structure of technology.

Virtualization

Virtualization allows the resources of a physical server to be shared among multiple virtual servers. Virtualization is not unique to cloud computing and can be used to share corporate resources among multiple processes and services, typically offering more efficient utilization of resources. For example, a single physical server can be used to host virtual machines (VMs) running an email server and a web server, saving the organization the cost of buying and running two physical machines. This resource sharing also makes it easier to move VMs between physical hardware, providing availability benefits.

Cloud computing takes the idea of server virtualization and expands it to virtualizing all aspects of an information system, including the basic infrastructure such as networking, compute, memory, physical data storage, data storage systems like databases, and even applications that traditionally ran on a user workstation. The CSP shares resources among a large number of services and customers (also called *tenants*). Each tenant has full use of their environment without knowledge of the other tenants. This increases the efficient use of the resources significantly.

Most CSPs have multiple locations providing the cloud services, and high-speed connectivity allows services and data to move seamlessly between locations. This allows the CSP to evenly distribute workloads, provides failover capabilities, and allows regulated customers to access cloud services in locations that meet their regulatory requirements.

The use of all-virtualized infrastructure can create some security and compliance concerns, such as data leaving a geographic area where it may not be governed by the same set of laws and regulations. These issues may be handled during contract negotiation, though most CSPs offer solutions designed with common regulations in mind. For example, AWS, Azure, and GCP all offer GDPR-compliant services that retain data in EU data centers and also offer solutions to the U.S. federal government that retain data only in U.S.-based data centers.

Virtualization relies on technology known as a *hypervisor*, which is software that governs access by VMs to the hardware resources. If the hypervisor is compromised, it could allow an attacker to gain access to other VMs running on the same hardware. This type of attack is known as an *escape*, and properly securing and patching the hypervisor is the responsibility of the CSP.

Early virtualization focused on creating multiple virtual computers on a single piece of physical hardware, which increased efficiency in resource utilization and offered portability for virtual machines (VMs). Containers are a more recent evolution of these virtualization concepts. A *container*, or *containerized application*, is an application packaged along with its required software dependencies and configuration information. A container platform, such as Docker, can be installed on any physical hardware and run any compatible containers. The containerized application is inherently more portable, as it can run on any platform so long as the container software is also installed.

Storage

A variety of storage solutions allow cloud computing to work. Two of these are storage area networks (SANs) and network-attached storage (NAS). These and other advances in storage allow a CSP to offer flexible and scalable storage capabilities.

A SAN provides secure storage among multiple computers within a specific customer's domain. A SAN appears like a single disk to the customer, while the storage is spread across multiple locations. This is one type of shared storage that works across a network. SANs utilize block-level storage, where data being stored is broken down into blocks of uniform size. Blocks can be stored more efficiently than files due to their uniform size, and the SAN software is responsible for arranging all the needed blocks when a specific piece of data is requested.

Another type of networked storage is the NAS. This network storage solution uses TCP/IP and allows file-level access. A NAS appears to the customer as a single file system similar to the hard drive in a workstation. Many operating systems offer native support for NAS using a variety of formats.

The responsibility for choosing the storage technology lies with the CSP and will change over time as new technologies are introduced. These changes should be transparent to the customer—from the customer's perspective, the access speed, integrity of data, and allocated storage space are the important factors, not the underlying storage technology. The CSP is responsible for the security of the shared storage resource, while customers retain responsibility for security data they store in the cloud.

Shared storage can create security challenges if data remnants are present on a disk after it has been deallocated from one customer and allocated to another. A customer has no way to securely wipe the drives in use or physically destroy them; typically a CSP will offer some form of secure deletion. However, customers can utilize a practice known as *crypto-shredding* to make these fragments unusable if recovered, by encrypting data and securely destroying the key.

Networking

As all resources in a cloud environment are accessed through the network, a robust, available network is an essential element. The Internet is the network used by public and community clouds, as well as many private clouds. This network has proven to be widely available with broad capabilities. The Internet has become ubiquitous in society, allowing for the expansion of cloud-based services.

An IP-based network is only part of what is needed for cloud computing. Low latency, high bandwidth, and relatively error-free transmissions make cloud computing possible. The use of public networks also creates some security concerns. If access to cloud resources is via a public network, like the Internet, the traffic can be intercepted, and if data is transmitted in the clear, it can be read. The use of encryption and secure transport keeps the data in motion secure and cloud computing safer. Some CSPs even offer dedicated connectivity into the edge of their network for organizations with a high volume of sensitive data that prefer not to utilize the public Internet for connectivity.

Databases

Databases allow for the storage and organization of customer data. By using a database in a cloud environment, the administration of the underlying database becomes the responsibility of the CSP, including key tasks such as patching, tuning, and other database administrator services. The exception is IaaS, where the user is responsible for whatever database they install.

The other advantage of databases offered through a cloud service is the number of different database types and options that can be used together. While traditional relational databases are available, so are other types. By using traditional databases and other data storage tools as well as large amounts of data resources, data warehouses, data lakes, and other data storage strategies can be implemented. The cost savings offered by the scale of cloud computing make big data applications such as these more affordable than they would otherwise be.

Orchestration

Cloud orchestration is the use of technology to manage cloud infrastructure. In a modern organization, there is a great deal of complexity, including a mix of on-premises infrastructure and multiple cloud services. Even small organizations are likely to have multiple cloud offerings, such as infrastructure hosted in a traditional CSP like AWS, GCP, or Azure, as well as SaaS applications used by the business like Google Workspace, GitHub, or Salesforce.

This complexity can lead to data being out of sync, processes being broken, and a fragmentation that leaves the IT department unable to keep track of all the cloud services, business processes, and data locations. Like the conductor of an orchestra, cloud orchestration partners keep all of these pieces working together including data, processes, and application services. Orchestration is the glue that ties all of the pieces together through programming and automation. Orchestration is valuable whether an organization runs a single cloud environment or a multi-cloud environment.

This is more than simply automating a few tasks. Automation is heavily used by cloud orchestration services to create one seemingly seamless organizational cloud environment. In addition to hiding much of the complexity of an organization's cloud environment, cloud orchestration can reduce costs, improve efficiency, and support the overall workforce.

The major CSPs provide orchestration tools. These include IBM Cloud Orchestrator, Microsoft Operations Management Suite (OMS), and AWS Cloud Formation. These offerings are typically best suited to manage their respective CSP's services. Organizations utilizing multiple CSPs can utilize multi-cloud orchestration tools to deploy infrastructure across various CSPs, such as Kubernetes.

Describe Cloud Reference Architecture

The purpose of a reference architecture (RA) is to allow a wide variety of cloud vendors and services to be interoperable and to provide consumers with guidance on optimal deployment of resources in the cloud. An RA creates a framework or mapping of cloud computing activities and cloud capabilities to allow the services of different vendors to be mapped and potentially work together more seamlessly. An example of this approach is the seven-layer Open Systems Interconnection (OSI) model of networking, which allows interoperability of networking protocols between different operating systems. As companies engage a wide variety of cloud solutions from multiple vendors, interoperability is becoming more important, and the reference architecture makes the process easier.

NIST provides a cloud computing reference architecture in SP 500-292, which was based on a Cloud Security Alliance (CSA) working group project for cloud enterprise architecture. CSA has continued to update material related to this RA, including mapping control frameworks to the RA providing guidance to security practitioners for securely deploying cloud services.

Some RA models like NIST are role-based and describe the activities needed to provision, use, and maintain cloud services. The NIST RA is intended to be vendor neutral and defines five roles: cloud consumer, cloud provider, cloud auditor, cloud broker, and cloud carrier. Other RAs, such as the IBM Cloud Computing Reference Architecture (CCRA), are layer-based, although they also identify key activities performed by cloud provider and consumer.

Cloud Computing Activities

Some organizations will be a mix of cloud consumer and cloud provider. Internal IT departments may migrate legacy computing environments to a private cloud model for consumption by the organization's users, while other services will be consumed strictly from external cloud providers; as an example, an organization might retain its on-premises Exchange environment while also consuming Microsoft 365 SaaS for collaboration. Cloud-native organizations are those with no traditional, on-premises IT environments. New organizations, such as startups, often pursue this model due to the ease of use, while some older organizations have