CCSP®

Official Textbook

Domain 1
Cloud Concepts, Architecture and Design

The CCSP Textbook is designed to accompany the Official ISC2 CCSP Certification Training and serves as your primary resource for the information covered in the CCSP learning experience.

An Official ISC2™ Publication

Table of Contents

Introduction	2
Overview	4
Objectives	6
Domain Content	7
Summary	131
Quiz	132
Terms & Definitions	144
Key Takeaways	151
Acknowledgments	157

Introduction

What does it take to effectively design, manage and secure data, applications and infrastructure in the cloud? CCSP addresses the essential domains of cloud security, from architecture and design to operations and compliance, and presents a comprehensive review of core concepts and industry best practices. It is intended for experienced professionals who want to strengthen and solidify their skills and knowledge in an ever-evolving industry.

ISC2 Code of Ethics

All information security professionals who are certified by ISC2 recognize that such certification is a privilege that must be both earned and maintained. All ISC2 members are required to commit to fully support the ISC2 Code of Ethics Canons. For more information on the Code of Ethics, please visit the ISC2 website.

ISC2 Code of Ethics Preamble
The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

Therefore, strict adherence to this Code is a condition of certification.

ISC2 Code of Ethics Canons
Protect society, the common good, necessary public trust and confidence and the infrastructure.

Act honorably, honestly, justly, responsibly and legally.
Provide diligent and competent service to principals.
Advance and protect the profession.

Get in Touch with Us

For more information about the CCSP certification and training, contact an Education Consultant in your region:

Americas
Phone: +1.866.331.4722 ext. 2
Email: training@isc2.org

Europe, Middle East and Africa:
Phone: +44 203 960 7800
Email: info-emea@isc2.org

Asia-Pacific:
Phone: +1.866.331.4722 ext. 2
Email: isc2asia@isc2.org
infoisc2-j@isc2.org (Japan)
isc2china@isc2.org (China)

Overview

The Cloud Concepts, Architecture and Design Domain is designed to provide certification candidates with knowledge of the building blocks necessary for the development of cloud-based systems. Candidates will be introduced to cloud computing concepts regarding the customer, provider, partner, measured services, scalability, virtualization, storage and networking. They will also learn about cloud reference architecture based on activities defined by industry-standard documents. Lastly, candidates will study relevant security and design principles for cloud computing and cost-benefit analysis of cloud-based systems.

1.1 Understand cloud computing concepts

1.1.1 Cloud computing definitions

1.1.2 Cloud computing roles and responsibilities

1.1.3 Key cloud computing characteristics

1.1.4 Building block technologies

1.2 Describe cloud reference architecture

1.2.1 Cloud computing activities

1.2.2 Cloud service capabilities

1.2.3 Cloud service categories

1.2.4 Cloud deployment models

1.2.5 Cloud shared considerations

1.2.6 Impact of related technologies

1.3 Understand security concepts relevant to cloud computing

1.3.1 Cryptography and key management

1.3.2 Identity and access control

1.3.3 Data and media sanitization

1.3.4 Network security

1.3.5 Virtualization security

1.3.6 Common threats

1.3.7 Security hygiene

1.4 Understand design Principles of Secure Cloud Computing

1.4.1 Cloud secure life cycle

1.4.2 Business continuity (BC) and disaster recovery plan (DR)

1.4.3 Business impact analysis (BIA)

1.4.4 Functional security requirements

1.4.5 Security considerations and responsibilities for different cloud categories

1.4.6 Cloud design patterns

1.4.7 DevOps security

1.5 Evaluate cloud service providers

1.5.1 Verification against criteria

1.5.2 System/subsystem product certifications

Objectives

- State the essential characteristics of cloud computing.
- Describe fundamental cloud computing services.
- Describe cloud computing reference architectures.
- Explain cloud computing activities.
- Compare cloud service capabilities and models.
- Describe cloud deployment models.
- Summarize economic characteristics of cloud computing.
- Summarize cloud computing security concepts.
- Describe key security considerations for each service model.
- Evaluate cloud computing ROI and KPI metrics
- Analyze key cloud service providers and identify the potential tools, frameworks and registries that evaluate them.

Understand Cloud Computing Concepts (1.1)

Objectives

- State the essential characteristics of cloud computing.
- Describe fundamental cloud computing services.

Overview

Although cloud computing drastically changes some of the traditional norms associated with information technology, much of the underlying technology has existed in some form for many years. This results in security concepts and principles that have existed for decades remaining valid, although they may differ in implementation. This material addresses many of those IT fundamentals and is designed to reinforce those foundational aspects that remain unchanged when cloud computing provisioning and consumption models are adopted.

Cloud Computing Definitions

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." — *National Institute of Standards and Technology (NIST) definition of Cloud Computing*

Cloud computing is the use of internet-based computing resources, typically "as a service" to internal or external customers, where scalable and elastic IT-enabled capabilities are provided. There are various definitions of what cloud computing means from NIST, Gartner and other leading standards bodies. The NIST definition above is the most commonly and globally used, being cited by professionals and others to clarify what the term "cloud" means.

Cloud Service Maturation

In the journey to cloud computing, information technology underwent many significant changes. To understand where we are now, it is important to understand where we have been. This brief history will clarify how enabling technologies of the cloud developed and were integrated into what is now defined as the cloud.

One fundamental cloud concept that dates to the 1950s, when modern computing was born, is the concept of time sharing. Early computers were massive, complex and expensive, and thus unaffordable for most would-be users. Time-sharing schemas permitted multiple programs to be run on the large computers of the time, each operating within discrete time slots. While the original implementations were manual, with operators exchanging one program for another, in the modern cloud infrastructure this concept is still in place, albeit heavily automated, allowing existing resources to be efficiently shared between many potential workloads running concurrently.

Interconnected networks (or the internet, as we now know it) emerged in the late 1960s and early 1970s. This permitted easier sharing of information and became an enabling technology for subsequent computer-use cases. Wide-ranging connectivity and dispersion of services became possible through connected computer networks and have steadily increased in capability since being introduced. As technology has advanced, previously separate networks converged into the Internet Protocol (IP) networks of the modern era with multiple service types coexisting on the same infrastructure.

Virtualization in one form or another has existed since IBM introduced the **virtual machine** (VM) operating system in the 1970s, which allowed multiple virtual systems to share a common physical implementation. At the time, the physical implementation was a single large mainframe, but advances in virtualization technology and computing infrastructure eventually allowed multiple virtual computers to operate on a single physical computer as well as allowing more powerful virtual systems to span multiple physical computing platforms. Virtualization has become a key component of any cloud infrastructure and is a key enabler for most other cloud technologies.

Easy and ubiquitous internet search engines and common web browser implementations that emerged in the 1990s enabled the delivery of both content and, more importantly, services through common interfaces (e.g., web pages). Computer users were able to obtain “online” services by locating a service provider and connecting to it using a web browser. This enabled companies to deliver services directly through web pages that could begin to emulate capabilities previously delivered through installed software packages.

During the late 1990s and early 2000s, mobility devices emerged and became commonly accessible with mobile access to networks using cellular and Wi-Fi services. Mobile computing in a practical form became the norm during this period, which necessitated services to which mobile devices could connect, regardless of location.

Data storage technologies have steadily evolved since the inception of modern computing. In most cases, they have grown in parallel with other technologies and have seen constant improvements in speed and capacity. In parallel with virtualization of processing, storage technologies developed that abstracted the physical storage media from the presentation of the storage. This has continued to evolve with modern cloud implementations to the point where physical storage can be accomplished using a wide variety of means while presenting standardized interfaces to the storage, some of which emulate traditional storage technologies (e.g., Storage Area Network [SAN], Network Attached Storage [NAS]), while others are unique to cloud implementations (e.g., some block storage mechanisms). As data storage solutions have dropped in cost over time, **cloud storage** of larger and larger amounts of data has become cost-effective.

As modern cloud capabilities emerged in the early 2000s, these various technological advances merged with the goal of producing highly efficient and cost-effective service offerings. As the modern cloud-computing cost models solidified, there also emerged a heavy reliance on shared infrastructure and variable pricing models, which are fundamental to the cloud concept now known as elasticity.

These concepts and others will be discussed in more detail throughout the course. While the core concepts of cloud computing have existed for many years, the modern implementation of cloud services extends and combines the legacy service

capabilities in ways that would not have been possible without the parallel advancement of supporting technologies and their implementation.

Roles and Sub-Roles

ISO/IEC 17789 cloud computing reference architecture defines three main roles for cloud computing:

Figure 1.1: ISO/IEC 17789 Roles and Sub-Roles

Cloud service customer (CSC): A party that is in a business relationship for the purpose of consuming cloud services.

Cloud service provider (CSP): A party that provides cloud services for consumers.

Cloud service partner (CSN): A party that is engaged in support of, or auxiliary to, activities of either the CSP, the CSC, or both. NIST uses the terms cloud service broker and cloud auditor, which both fall under this ISO/IEC 17789 role.

More information about roles and their activities is included in Domain 1.2.

Technology Implementation Options

Cloud computing can take many forms to solve any problems. There are a wide variety of use cases for cloud computing and cloud-based technologies. There is no single answer to what the cloud can do for its users, as it provides a spectrum of choices. Thus, cloud consumers face a variety of choices and selections on offer from cloud providers that can be put together in many configurations to produce seemingly infinite solutions.

Spectrum of Different Cloud Services

Cloud services provide a wide spectrum of service offerings. This course covers the higher-level offerings (e.g., compute, storage, network), but individual CSPs will have specific offerings and may provide unique combinations of offerings.

In addition to the traditional compute, storage, and networking services offered by most CSPs, many also offer services that have been developed or optimized for particular customer-use cases. These services often combine the CSP's compute, storage, and networking capabilities with specialized automation (orchestration) or preconfigure aspects of the service to optimize them for specific use cases.

For example, the following list includes cloud offering categories available in the **product catalogs** of major CSPs:

- IAM
- Monitoring and anomaly detection
- Helpdesk/customer support (CSP to Cloud Customer and Cloud Customer to their customer)
- Database services
- Various storage offerings
- Various machine learnings
- Data discovery services
- Load balancing
- Content delivery network
- Web application firewalls
- API and XML gateways
- Machine learning and AI

Cloud Computing Characteristics

As stated earlier, cloud computing is 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 following essential characteristics of cloud are a rule book, or a set of laws when identifying cloud services or discussing how a cloud service can be used. Where a service or solution does not meet all the following key characteristics, it is not genuine cloud computing. Both ISO/IEC 17788 and NIST cite the following as key characteristics of cloud computing.

On-Demand Self-Service

On-demand self-service refers to cloud service that enables the provision of cloud resources on demand (i.e., whenever and wherever they are required). From a security perspective, this has introduced challenges to governing the use and **provisioning** of cloud-based services, which may violate organizational policies. By its nature, on-demand self-service does not require procurement, provisioning, or approval from finance, and as such can be provisioned by anyone with a credit card or valid method of payment and at least minimal identity checking.

Self-service, also referred to as "self-provisioning," is the process by which the customer or user can provision, manage, or operate cloud services without interaction or assistance from the cloud provider or its personnel. Additionally, all operations and functions should be available for the user to select or configure, based on the cloud service type, through completion of the user or system activities.

Broad Network Access

The cloud, by its nature, is always on and always accessible, offering users widespread access to resources, data and other assets. Access what you want, when you need, from any location. In theory, all you should require is internet access and relevant credentials and tokens, which will give you access to the resources.

The interesting dynamic of recent times is the mobile device and smart device revolution, which is altering the way organizations fundamentally operate. These devices should be able to access the relevant resources; however, compatibility issues, the inability to apply security controls across all variations, and nonstandardization of platforms and software systems have stemmed this. This has also led to potential concerns over the trustworthiness of devices connected to cloud services.

Multitenancy

Multitenancy refers to a cloud environment where multiple entities (tenants) use an architecture in which a single instance serves multiple customers. While tenants

may be given the ability to customize some components of the application or service, they cannot customize the relevant code or service for other tenants. With multitenancy, each tenant's data is isolated from, and not visible or accessible to, other tenants.

Resource Pooling

Resource pooling is another advantage of cloud computing. In the past, when more compute power was needed, IT would turn to finance and procurement and embark on a lengthy and costly process. Often, these systems could utilize the resources between 80-90% for a few hours a week and reside at an average of 10-20% for the remainder. In contrast, the cloud pools resources for use across the user landscape or multiple clients, which can then be scaled and adjusted to the user's or client's needs based on their workload or resource requirements. Cloud providers typically have large numbers of resources available, from hundreds to thousands of servers, network devices and applications, that can accommodate many customers and can prioritize and facilitate appropriate resourcing for each client.

Rapid Elasticity

Rapid elasticity, which invokes the image of a band that can be pulled and stretched, allows the user to obtain the additional resources, storage and compute power that its specific need or workload requires. This is most often transparent to the user, with more resources added seamlessly as necessary. Cloud services use the pay-per-use concept, which is of particular benefit to seasonal or event-holding businesses utilizing cloud services. Think of a provider selling 100,000 tickets for a major sporting event or concert. Leading up to the ticket release date, little or no compute resources are needed; however, once the tickets go on sale, they may need to accommodate 100,000 users in the space of 30 to 40 minutes. In this case, rapid elasticity and cloud computing are beneficial compared to traditional IT deployments that heavily use capital expenditure (CapEx) to gain the ability to support such demand.

Measured Service

Cloud computing offers this unique, key component that traditional IT deployments have struggled to provide. Resource usage can be measured, controlled, reported, and alerted upon, which results in multiple benefits and overall transparency between the provider and client. In the same way that consumers may have metered electricity service or credit-reloadable mobile phones, these services facilitate the awareness and control of costs. Users pay for what they use and can get an itemized bill or breakdown of use.

A key benefit for proactive organizations is the ability to charge departments or business units for their use of services, thus allowing IT and finance to quantify exact usage and costs per department or by business function—something that was incredibly difficult to achieve in traditional IT environments. While measured service is certainly a part of most cloud services to permit the CSP to bill for use, it may also provide cloud consumers useful insight into actual service consumption.

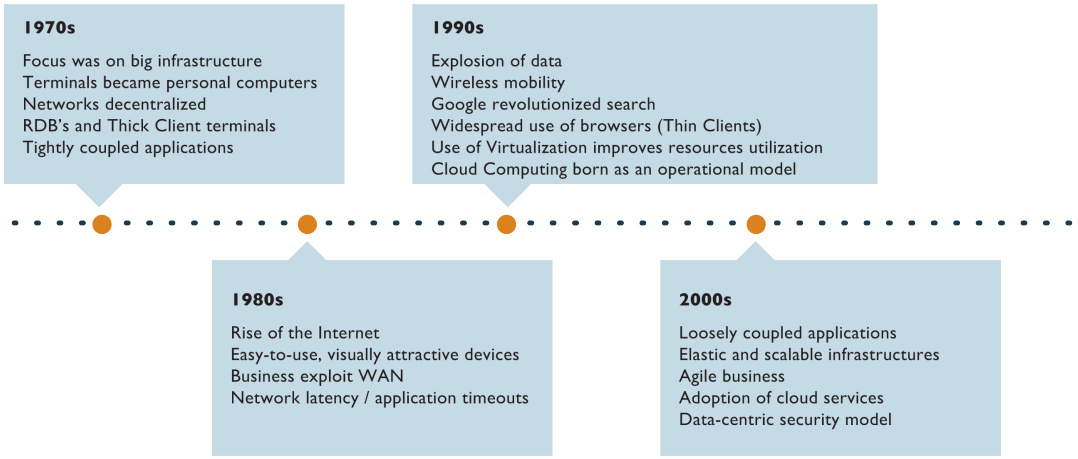


Figure 1.2: Evolution of IT Service Maturation

Building Block Technologies

Cloud computing is a unique economic, operational and business model. It does not, however, change the fundamentals of technology or security. Although standardization and automation drive revolutionary change in those three

domains, fundamentally, cloud computing still delivers compute, storage and networking services.

Compute Services

Compute services combine central processing units (CPUs), memory and ephemeral storage capabilities using virtual machines (VMs). A VM is a computer file, called an image, that emulates a real computer. The environment is segregated from all other cloud users. The VM is sandboxed and cannot be used to access the underlying physical computer. Multiple VMs operate on the same physical computer simultaneously. This reduces costs and physical hardware quantities, associated maintenance costs, power consumption, and data center cooling requirements. Virtual servers scale quickly but may have reduced performance when compared to directly using a single-tenant physical server. CSPs usually provide a choice of operating systems (e.g., Linux, Microsoft Windows, Solaris). VMs can also have varying numbers of computing cores and variable amounts of RAM and quantities of storage, all of which may run with variable performance specifications (e.g., speed, bandwidth). Autoscaling is used to automatically change the resources assigned to a workload, allowing for cloud capabilities that grow or shrink as actual usage or needs change.

Storage Services

Storage services are either ephemeral (as provisioned with VMs) or persistent. Persistent storage remains available after a VM is deprovisioned and is normally backed by mechanical hard disk drives or solid-state drives. The most used types of persistent storage services are file, block and object. File-level storage will typically have similar functionality to a hard drive or server share in a traditional environment where arbitrarily sized files can be stored, and the storage system determines the specific mechanics for doing so. Block storage is analogous to how data is stored on a physical hard drive, in that data is stored in fixed size blocks. Block storage can be used by applications to efficiently store and retrieve bulk data and provides more optimization possibilities at the application level than file storage. However, it requires more information at the application level to store and retrieve the appropriate data blocks. Object or blob (binary large object) storage allows storing arbitrary binary objects without any predefined structure or hierarchy. It offers the storing application the most flexibility and can be simple to

use but provides a more limited structure that can be a disadvantage in certain use cases. Object storage can be used for any use case, including the storage of logs, application data, audio and video content.

Failure tolerance in a storage offering is provided through duplication of data element copies across the cloud environment. If a copied version is lost, data is still recoverable from the other copies. Storage consistency is a fundamental concept in cloud computing and describes the time it takes for all data copies to be the same. Strict consistency ensures that all copies of the data have been duplicated among all relevant copies before finalizing the transaction to increase availability. In eventual consistency, the consistency of data is relaxed, which reduces the number of replicas that must be accessed during read and write operations before the transaction is finalized. When using eventual consistency, data changes are eventually transferred to all data copies through asynchronous propagation via the network.

Some providers also offer key-value storage that delivers higher availability and performance. This service distributes data across different IT resources and locations and can meet more flexible data structure requirements. This can be used to satisfy regulatory or legal data retention requirements.

Networking Services

Networking services connect cloud components to provide elastic infrastructures and platforms. They rely on physical network hardware that has been virtualized into a software-defined network (SDN). Physical components (e.g., networking interface cards [NICs], switches, routers) are abstracted into virtualized equivalents that can be managed by CSP customers. By using a self-service interface, customers can design, implement and configure virtual circuits, firewalls, load balancers, network address translations (NATs), and network cross-connects. They can also isolate groups of virtual components into security groups. The security group construct is used to control communications ports, protocols, virtual local area networks (VLANs), and virtual wide area networks.

Critical CSP management functions are conducted over three planes referred to as the management plane, control plane, and data/forwarding plane. The management plane is used to provision, configure, and deprovision all cloud

resources to external and internal CSP customers. The control plane connects provisioned resources to each other in segregated networks as specified by each individual tenant. The data or forwarding plane is used to transfer individual tenant data to and from that specific tenant's provisioned virtual compute and storage resources.

Virtualization

Virtualization is any technology or set of technologies that separates the presentation of a service or capability from the physical infrastructure that supports it. Virtualization is a key component of any cloud service at one or more layers. Computer, storage, and network services can all be virtualized so that service presented to a consumer is abstracted from the underlying physical infrastructure. Virtualization allows the CSP to manage the physical infrastructure based on overall capacity, distribution, redundancy, and reliability requirements, while delivering a consistent service or capability to the cloud consumer. Changes to the physical infrastructure will have minimal or negligible impact on the service or capability provided to the consumer.

Virtualization also supports dynamic provisioning and deprovisioning of physical assets to support services and is a key component of cloud elasticity. This allows the service or capability offerings presented to a cloud consumer to expand when required to support workloads or shrink when not utilized, while the consumer is presented with a consistent and standardized interface to the service or capability.

Figure 1.3: Example Global Cloud Service Provider

Databases

Data storage and data storage services are key components of the cloud. While storage comes in many forms, it is often desirable to have ordering to the storage to find and extract data elements on demand. Storage capabilities can also be accessed using CSP-provided **cloud database** services. These PaaS offerings normally align as either a relational form Structured Query Language (SQL) or nonrelational (NoSQL) type. SQL relational databases handle data comprising large numbers of similar data elements. These elements have specified dependencies among each other. Users make specific assumptions regarding the data structure and the relationship consistency between the retrieved data elements when this structured data is queried. Data elements are recorded in tables and columns that

represent data element attributes. Table columns may also enforce dependencies for how entries in one table column relate to a corresponding column in a different table. These dependencies are strictly enforced. In NoSQL databases (e.g., Cassandra, Mongo, MapReduce), there is no enforced database structure. The data manipulation process is split up and mapped to multiple application components. As distributed applications are scaled out, data processing is similarly distributed among multiple components. The data processing components simultaneously execute the query to be performed on assigned data chunks. Processing results are consolidated into a single result data set.

Cloud Orchestration

The CSP operational process responsible for receiving, fulfilling, managing, monitoring and metering customer services across all portions of the cloud infrastructure is referred to as **cloud orchestration.** The CSP software components in aggregate responsible for orchestration is called the **cloud operating system (OS).** The OS for each CSP will be unique to their specific service offerings, although they may use the same or similar building blocks. Orchestration is accomplished using hardware, software, and service application programming interfaces (APIs). The orchestration layer for many CSPs will include mechanisms to allow cloud consumers to access information or make requests for services, which is a key component of the self-service cloud characteristic.

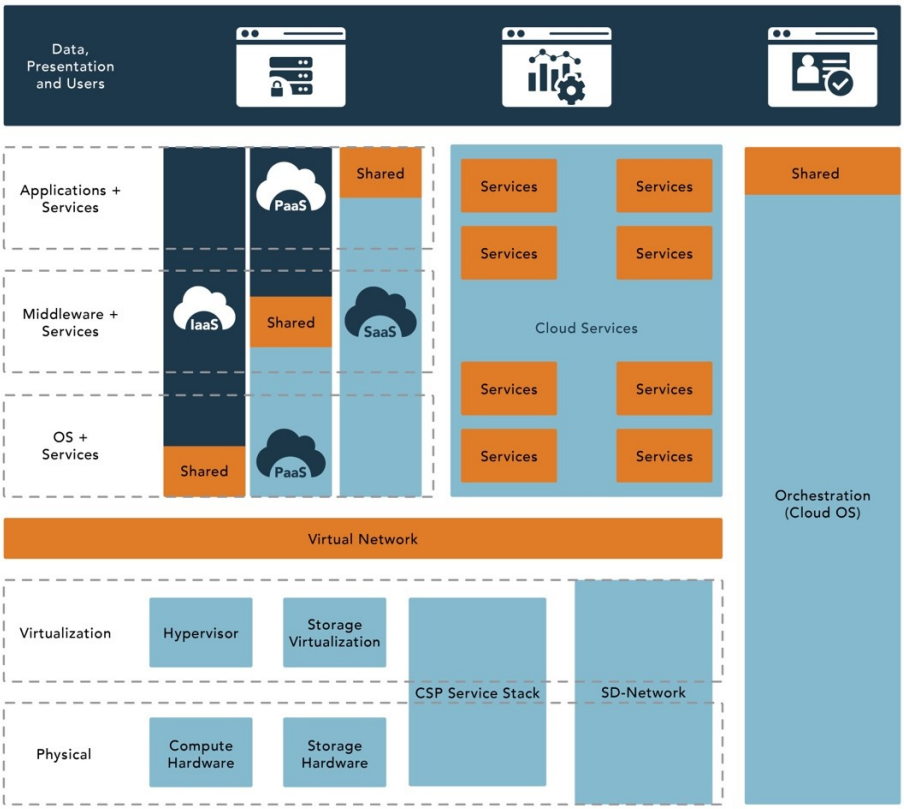


Figure 1.4: Generic CSP Architecture

Key Drivers for Cloud Computing

The key driver for cloud computing is the shift from CapEx, where organizations had to invest large sums of money, to operational expenditure (OpEx), which now enables companies to pay per use and avail themselves of pricing structures similar to monthly or quarterly leasing agreements. Additional drivers include but are not limited to:

- *Scalability.* Users have access to many resources that scale in response to user demand.
- *Elasticity.* The environment transparently manages a user's resource utilization based on dynamically changing needs.
- *Cost.* The pay-per-usage model allows an organization to pay only for the resources they need with no investment in the physical resources available in the cloud. There are no infrastructure maintenance or upgrade costs.

- *Mobility.* Users can access data and applications from around the globe.
- *Collaboration.* Users can see files in the cloud and work simultaneously on common data and information.
- *Risk reduction.* Customers can use the cloud to test ideas and concepts before making major investments in technology.

Describe Cloud Reference Architecture (1.2)

Objectives

- Describe cloud computing reference architectures.
- Explain cloud computing activities.
- Compare cloud service capabilities and models.
- Describe cloud deployment models.
- Summarize economic characteristics of cloud computing.

Overview

Implementing a secure design when creating a data center involves many considerations. Prior to making design decisions, the organization should identify all compliance requirements for its cloud infrastructure and services, whether developed as a service provider or consumer. When designing a capability for public cloud services, consideration should be given to the levels of security that will be offered to the customer. For example, if customers host payment card industry data, then those standards should be included in the design. The location of the physical infrastructure and the potential consumers of the cloud service will also impact compliance decisions. Legal and regulatory requirements differ based on the geographic location of the provider and consumers. Both cloud providers and consumers should have a clear understanding of these requirements at the national, state/province, and local level within the geographic locations involved in any service design.

Two reference architectures are widely used by organizations to design and assess cloud services and infrastructure:

- NIST Cloud Computing Reference Architecture and Taxonomy
- ISO/IEC 17789 Cloud Computing Reference Architecture (CCRA)
- A CCSP should be familiar with both as summarized in the following sections.

Architectures and Frameworks

Reference architectures and frameworks provide structure for development of capabilities and the expression of capabilities in a standardized format. Reference architectures and frameworks come in many different forms, but they embody best practices and what are essential components of an industry, technology, or service capability. They can be used to guide the development of new capabilities or help with the assessment of an existing capability. Reference architectures and frameworks also help to make complex structure more understandable by breaking it down into component pieces.

The two reference architectures to be discussed in this section, NIST Cloud Computing Reference Architecture and Taxonomy and ISO/IEC 17789 CCRA, are specific to the cloud and help organize the components of a cloud architecture into a set of common elements using common terminology. While both reference architectures cover the cloud, they differ in the approach and level of detail. However, both reference architectures contain significant similarities and complement each other in some ways.

Specific frameworks for applying risk reduction mechanisms have also been developed that help framework users to consistently apply standardized risk reduction mechanisms across multiple technologies. These risk reduction mechanisms are commonly referred to as **controls**. Domain 1.3 will include more detail on control frameworks that provide standardized structure for identifying, applying and assessing the effectiveness of security controls across multiple technologies or environments.

Cloud Computing: ISO/IEC 17789 vs. NIST

Although the cloud computing reference models offered by ISO/IEC and NIST are used to address the same IT-as-a-Service model, they can be confusing. These two standards are important because of their widespread use and the need for CCSPs to be knowledgeable of each.

The table shows the differences in terminology and focus. The components will be described in the following section, but the table is an easy reference for comparing the two cloud standards.

Item	ISO/IEC 17789	NIST
Cloud Computing Systems Description	Viewpoints (User, Functional, Deployment, Implementation)	Interaction between Actors
Cloud Computing Functional Components	Functional Layers	NIST Reference Model
Cloud Ecosystem Participants	Roles and Sub-Roles	Actors
IT Services Consumed by Cloud Customers	Cloud Service Capabilities and Categories	Cloud Service Models
Cloud Ecosystem Governance Model	Cloud Deployment Models	Cloud Deployment Models

Table 1.1 Cloud Computing: ISO/IEC 17789 vs. NIST

Under ISO/IEC 17789, roles are divided into **sub-roles** and are associated with activities:

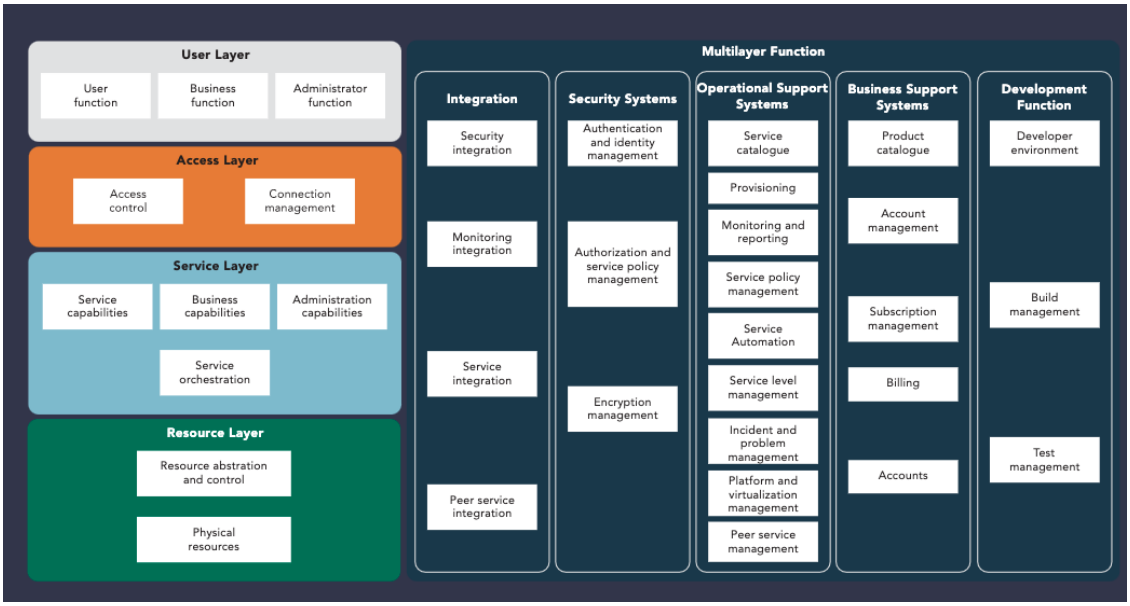


Figure 1.5: Functional Layers

Here are NIST reference models to compare with the ISO/IEC 17789 reference model. These models will be explored in depth later.

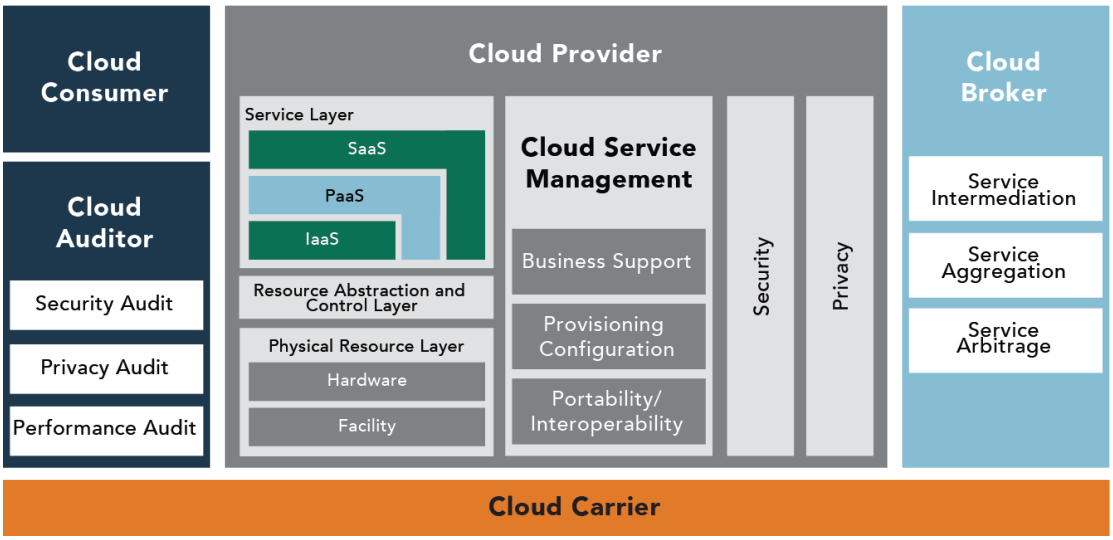


Figure 1.6: NIST Reference Model

ISO/IEC 17789 Cloud Computing Reference Architecture (CCRA)

This listed reference architecture, originally published in 2014, was reviewed and confirmed in 2021 and remains current. It includes several key components that require comprehensive review and understanding to determine which controls and techniques may be required to address the logical, physical, and environmental cloud-computing design.

ISO/IEC describes cloud computing systems from four distinct viewpoints:

- *User view.* This includes the system context, the parties, the roles, the sub-roles and the cloud computing activities.
- *Functional view.* This includes the functions necessary for the support of cloud computing activities.
- *Implementation view.* This includes the functions necessary for the implementation of a cloud service within service parts and/or infrastructure parts.

- *Deployment view.* This shows how the functions of a cloud service are technically implemented within already existing infrastructure elements or within new elements to be introduced in this infrastructure.

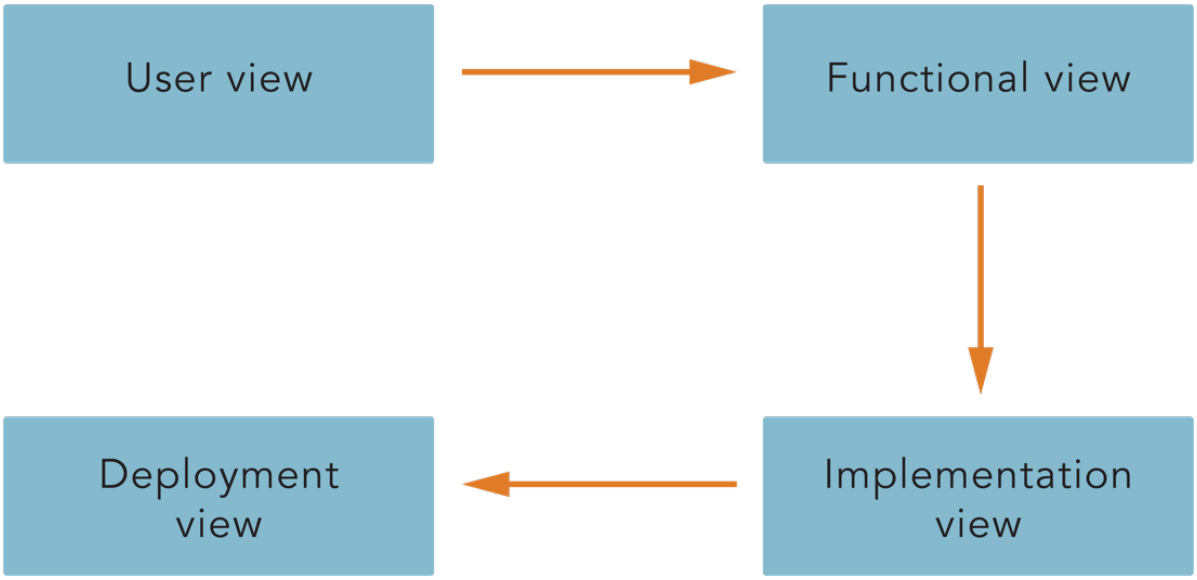


Figure 1.7: ISO/IEC 17789 Cloud Computing Viewpoints

The ISO/IEC 17789 implementation and deployment views are specific to technology and vendor-specific implementations. Because of this, they are considered out of the scope for the international standard. For CCRA purposes, only user and functional views are defined as "within scope."

The below figure shows an example mapping defined roles (people), activities performed by the roles and functional (technical or process) components of the architecture. A completed architecture would map the relationships and interactions among all roles, activities and functional components.

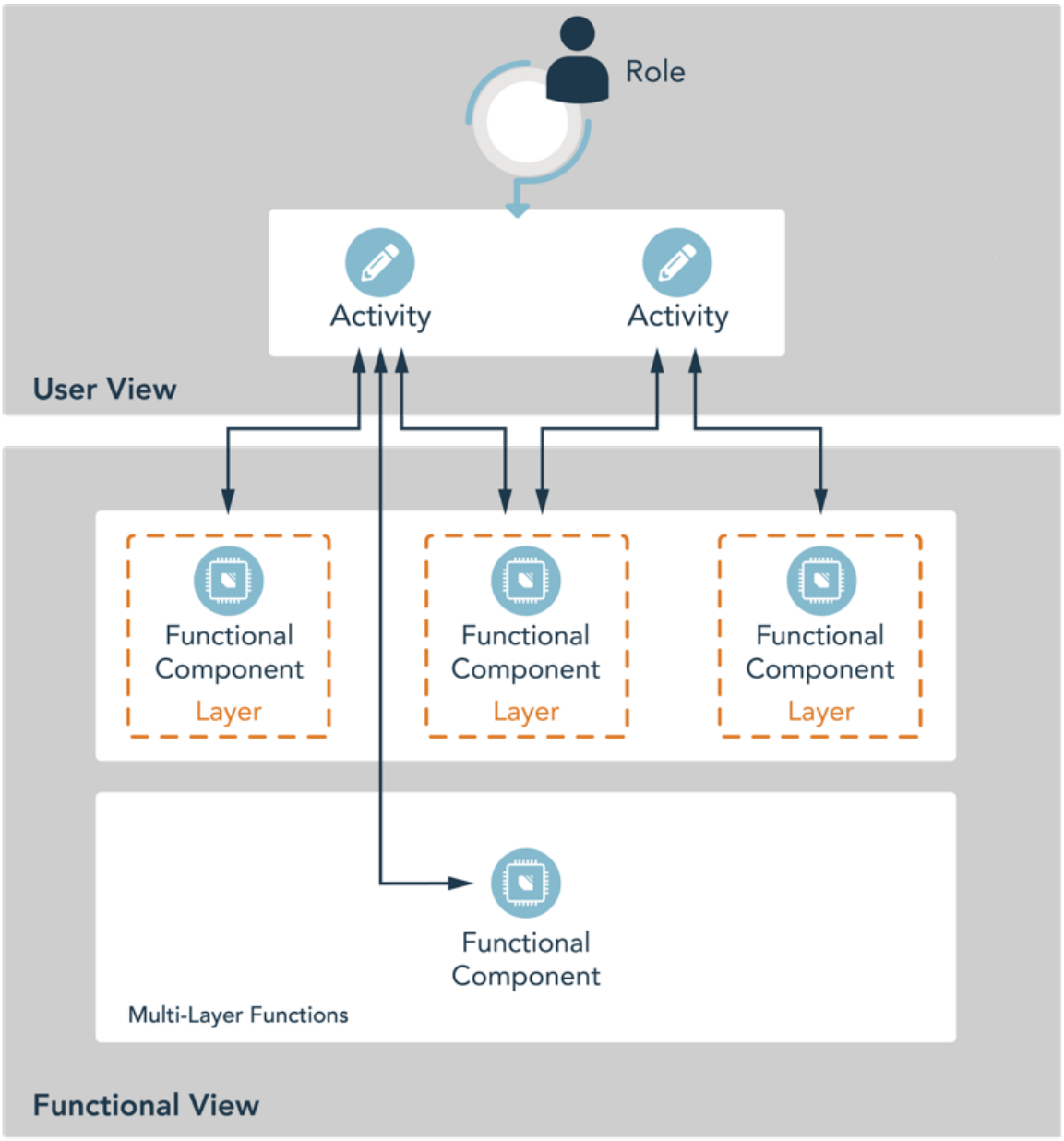


Figure 1.8: ISO/IEC 17789 User View to Functional View

The following diagram shows a basic relationship between roles, sub-roles, activities, and functional components of the architecture framework. The views combine architectural elements together to describe some relationship or sets of related activities.

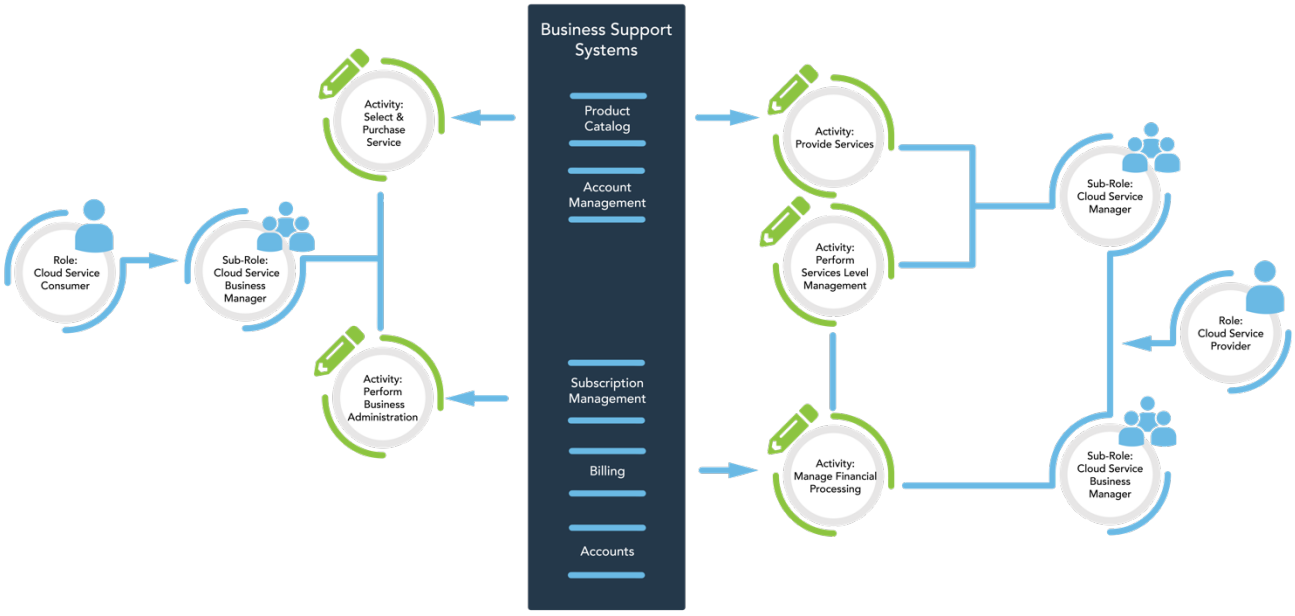


Figure 1.9: ISO/IEC 17789 Relationships of the Architecture Framework

The ISO/IEC 17789 cloud computing user view addresses cloud computing activities, roles and sub-roles, parties and cross-cutting aspects. These will be addressed in later sections.

The ISO/IEC 17789 cloud computing functional view described in the figure above is similar to the NIST reference model in that the high-level set of functional components is presented.

Cloud Computing Activities

With traditional computing and technology environments, there are several activities that are essential for creating, designing, implementing, testing, auditing and maintaining the relevant assets. ISO/IEC 17789 links cloud computing activities to traditional technology environment activities using sub-role activities.

Figure 1.10: Cloud Service Partner (CSN)

A Cloud Service Partner is generally responsible for a number of activities, which include:

- *Design, create and maintain service components.* The partner designs and creates software components as part of the implementation of a service. It will also process problem reports and provide fixes to software and enhancements to service implementations.
- *Compose services.* The partner develops new services by combining or modifying existing cloud services.
- *Test services.* The partner tests the components and services created by the cloud service developer.
- *Perform audits.* The partner requests or obtains audit evidence and conducts any required tests on the system being audited and obtains evidence programmatically.
- *Report audit results.* The partner provides documentation of the results of any requested or required audit.
- *Acquire and assess customers.* The partner markets and sells cloud services with the result that a cloud service customer contracts to use one or more services.
- *Assess marketplace.* The partner evaluates the current cloud computing marketplace to identify and recommend services that allow customers to meet their business goals.
- *Set up legal agreements.* The partner establishes the service agreement between the customer and the chosen providers.

Cloud service user
- Use cloud service

Cloud service administrator
- Perform service trial
- Monitor service
- Administer service security
- Provide billing and usage reports
- Handle problem reports
- Administer tenancies

Cloud service business manager
- Perform business administration
- Select and purchase service
- Request audit report

Cloud service integrator
- Connect ICT systems to cloud services

Figure 1.11: Cloud Service Customer (CSC) Activities

- The Cloud Service Customer is generally responsible for a number of activities, which include:
- *Use cloud service activity.* The customer accomplishes critical security tasks and other tasks utilizing the services of the provider.
- *Perform service trials.* The customer uses the services of a provider to ensure that the cloud service provided is appropriate for their business needs.
- *Monitor service.* The customer is responsible for monitoring the quality of the delivered service with respect to service levels as defined in the service-level agreement (SLA).
- *Administer service security.* The customer ensures appropriate security for its data, including data backup and recovery, administering security policies, defining encryption and integrity technologies and defining the handling of any personally identifiable information (PII).
- *Handle problem reports.* The customer performs customer-side handling of any reported problems that arise from the use of cloud services.
- *Administer tenancies.* The customer administers its tenancies with the provider.
- *Perform business administration.* The customer manages the business aspects of the use of cloud services, including accounting and financial management.

- *Select and purchase services.* The customer examines the cloud service offerings to determine whether they meet its business and technical requirements.
- *Request audit reports.* The customer requests relevant reports of an audit of the cloud service, typically conforming to a particular audit standard as agreed upon in the SLA.
- *Connect ICT systems to cloud services.* The customer is responsible for the integration of existing ICT systems and cloud services, connecting existing ICT components and applications with the target cloud services, and connecting its monitoring and management systems with the provider's monitoring and control of cloud services.

Cloud service operations manager
- Prepare systems
- Monitor and administer services
- Manage assets and inventory
- Provide audit data

Cloud service deployment manager
- Define environment and processes
- Define and gather metrics
- Define deployment steps

Cloud service manager
- Provide services
- Deploy and provision services
- Perform services level management

Cloud service business manager
- Manage business plan
- Manage customer relationships
- Manage financial processing

Customer support and care representative
- Handle customer requests

Intercloud provider
- Manage peer cloud services

Cloud service security and risk manager
- Manage security risks
- Design and implement service continuity
- Ensure compliance

Network provider
- Provide network connectivity
- Deliver network services
- Provide network management services

Figure 1.12: Cloud Service Provider (CSP) Activities

A Cloud Service Provider is generally responsible for a number of activities, which include:

- *Prepare systems.* The provider prepares the infrastructure in its environment for new cloud service deployments.
- *Monitor and administer services.* The provider monitors and administers services and their associated infrastructure, including user and system privileges.
- *Manage assets and inventory.* The provider tracks all compute, storage, network and software assets and the relationship between them. It is also responsible for onboarding new assets and safe disposal of assets that are no longer needed.
- *Provide audit data.* The provider collects and provides relevant data in response to an audit request, including data relating to security controls or service performance.

- *Define environment and process.* The provider defines and maintains the required technical environment and operational processes used when a service is running.
- *Define and gather metrics.* The provider defines service-level metrics and management.
- *Define deployment steps.* The provider defines the steps required for the deployment of services.
- *Provide services.* The provider performs all steps required to deliver a cloud service to its customers.
- *Deploy and provision services.* The provider is responsible for implementing services and making them available at a network end point accessible to the customer in such a way that the customer can handle service requests from users.
- *Perform service-level management.* The provider is responsible for compliance with SLA targets.
- *Manage business plan.* The provider defines a service offering and creates a business plan to provide cloud services to customers. It will track the sales and service usage against the business plan and prepare and adjust the plan as needed to provide cloud services.
- *Manage financial processing.* The provider handles billing and the receipt of payments from the customer.
- *Handle customer requests.* The provider handles support requests and responds to reports and incidents.
- *Manage peer cloud services.* The provider manages the usage of cloud services of a peer cloud service provider, if applicable.
- *Manage security and risks.* The provider manages security and risks associated with the development, delivery, use and support of its services.
- *Design and implement service continuity.* The provider considers the potential for failure of a cloud service and its supporting infrastructure and establishes appropriate response plans and recovery processes to maintain the cloud service's availability within the terms of the SLA.
- *Ensure compliance.* The provider is responsible for regulatory and standards compliance.
- *Provide network connectivity.* The provider establishes requested network connections and related capabilities, including connections between the

customer and the provider's system and between one provider's system and another customer's system, as required.

- *Deliver network services.* The provider provides required or requested network-related services, such as firewalls or load balancing.
- *Provide network management services.* The provider manages the network infrastructure used to carry cloud services.

ISO/IEC Cloud Capability Types and Cloud Service Categories

ISO/IEC 17788 defines Cloud Capability Types and Cloud Service Categories as part of the ISO Cloud model. The ISO model can be confusing; however, the ISO/IEC 17788 definitions for the three primary cloud service categories relate directly to the three cloud capability types and are consistent with the NIST definitions. The CCSP should recognize the different terminology used in the ISO/IEC 17788 and in NIST cloud references and be able to relate the terminology to core cloud concepts and commonly used terminology.

The following sections will cover the capability types and service categories in more detail. For **Infrastructure as a Service** (IaaS), **Platform as a Service** (PaaS), and **Software as a Service** (SaaS), the definitions and descriptions provided will cover both the ISO/IEC 17788 and NIST usage of those service categories.

ISO/IEC Cloud Capability Types and Cloud Service Categories	
ISO/IEC Cloud Capability Types are: • Infrastructure Capability Type • Platform Capability Type • Application Capability Type	ISO/IEC Cloud Service Categories are: • Communications as a Service (CaaS) • Compute as a Service (CompaaS) • Data Storage as a Service (DSaaS) • Infrastructure as a Service (IaaS) • Network as a Service (NaaS) • Platform as a Service (PaaS) • Software as a Service (SaaS)

Table 1.2: ISO/IEC Cloud Capability Types and Cloud Service Categories

Cloud Capability Types

ISO/IEC 17788 defines cloud capability types as a classification of the functionality provided by a cloud service provider to the cloud service customer, based on the resources used. There are three different cloud capability types:

- *Application capabilities type.* A cloud capabilities type in which the cloud service customer can use the cloud service provider's applications.
- *Platform capabilities type.* A cloud service capabilities type in which the cloud service customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more executing environments supported by the cloud service provider.
- *Infrastructure capabilities type.* A cloud capabilities type in which the cloud service customer can provision and use processing, storage, or networking resources.

While defined by ISO, the cloud capability types are less commonly used to describe cloud services, but are analogous to the IaaS, PaaS, and SaaS terms that are typically used.

Cloud Service Categories

The ISO/IEC 17788 also defines cloud service categories that possess a common set of qualities. Within this list, the typically used IaaS, PaaS, and SaaS are included, along with some lesser-used examples of other cloud service categories. Note that the definitions for IaaS, PaaS, and SaaS essentially refer to the related capabilities type, so in practice they are often used synonymously. The CCSP should recognize that the ISO standard does differentiate between capability types and service categories, but that for IaaS, SaaS, and PaaS, that category and capability are the same.

Representative cloud service categories are:

- *Communications as a Service (CaaS).* A cloud service category in which the capability provided to the cloud service customer is real-time interaction and collaboration.
- *Compute as a Service (CompaaS).* A cloud service category in which the capabilities provided to the cloud service customer are the provision and use of processing resources needed to deploy and run software.
- *Data Storage as a Service (DSaaS).* A cloud service category in which the capability provided to the cloud service customer is the provision and use of data storage and related capabilities.
- *Infrastructure as a Service (IaaS).* A cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type, so that the cloud service customer can provision and use processing, storage or networking resources.
- *Network as a Service (NaaS).* A cloud service category in which the capability provided to the cloud service customer is transport connectivity and related network capabilities.
- *Platform as a Service (PaaS).* A cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type, in which the cloud service customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more executing environments supported by the cloud service provider.
- *Software as a Service (SaaS).* A cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type.

While the ISO definitions for capability types and service categories can be confusing, most references recognize IaaS, PaaS, and SaaS as the most common, high-level description for cloud services. These are the service categories that are consistent with the capability types defined under ISO, and the definitions are equivalent to the NIST definitions for IaaS, PaaS, and SaaS.

Application Capabilities

SaaS cloud computing reduces or removes the large up-front capital investment required for development, which makes the possibilities nearly endless for

organizations to create and operate applications that may not have been practical without it. In addition to secure access via the internet, cloud computing also allows for scalability to run and execute programs using flexible capacity for computing and storage, which brings additional value to the developers.

SaaS cloud computing brings many other benefits as well, including reducing hardware and software costs and simplifying application licensing, since most hardware and underlying software is leased rather than purchased. Support costs are also reduced, as the infrastructure support is included in the cost of cloud services.

Other benefits of SaaS include:

- *Cost reduction.* SaaS cloud deployments reduce the need for high-end hardware, such as servers and large storage arrays. It is also no longer necessary to provide hardware for redundancy.
- *Software and application licensing.* In a SaaS deployment, capital expenses are no longer needed for software to provide virtualization services. This software is included in the cloud provider's costs and is licensed on an as-needed basis rather than a one-time up-front expense.
- *Reduced support costs.* All support costs related to the hardware and virtualization are the responsibility of the cloud service provider. Therefore, these costs are often spread across multiple customers, reducing the operating expense for each customer.

Platform Capabilities

PaaS allows organizations to manage and deliver software that can be customized in the following areas:

- *Support for multiple languages and frameworks.* The platform enables developers to write code in their preferred language, including many open-source frameworks; that allows portability between cloud service providers.
- *Multiple environments.* Applications that are built on PaaS cloud platforms offer the ability to easily migrate between public cloud, private cloud, and even local hypervisors to facilitate contingency and continuity planning. This ensures the application will remain available in nearly any situation.
- *Choice.* Customers can develop and run applications in many types of environments, contributing to the portability that makes PaaS desirable for many businesses.
- *Autoscale capabilities.* In a PaaS environment, the platform can assign and reassign system resources as needed to support fluctuations in workload. This is especially helpful to organizations that experience heavy and light workloads during a cycle.

Infrastructure Capabilities

IaaS reduces the overall cost of hardware in the organization while allowing the most granular control of systems and infrastructure for the cloud customer. IaaS reduces the costs associated with hardware and the direct maintenance of the hardware, yet still requires significant investment in skilled resources. The following infrastructure characteristics remain:

- *Scale.* Automation and tools to add and remove components of infrastructure as needed to fill the customer's needs with no barriers or restrictions.
- *Converged network.* The ability to provide services without regard to network boundaries and without the need for additional networking resources.
- *On-demand self-service capacity.* A customer portal gives the customer visibility into the IaaS environment, allowing the customer to add, remove, manage, and review all resources in use without intervention by the provider.

- *Resilience and high availability.* IaaS providers automatically move resources across multiple pieces of hardware across multiple geographic locations, which results in a high level of resilience for the cloud customers.

NIST Cloud Computing Reference Architecture and Taxonomy

The NIST Cloud Computing Reference Architecture and Taxonomy was designed to accurately communicate the components and offerings of cloud computing. The guiding principles used to create the reference architecture were:

- Develop a vendor-neutral architecture that is consistent with the NIST definition.
- Develop a solution that does not stifle innovation by defining a prescribed technical solution.

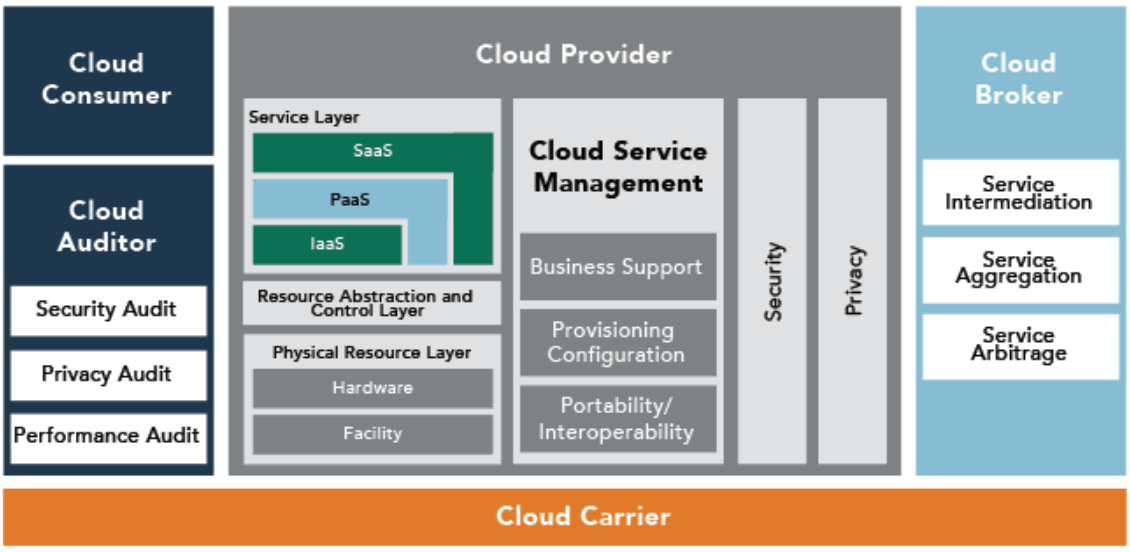


Figure 1.13: NIST Reference Model

Actors in Cloud Computing

The NIST cloud computing reference architecture defines five major actors. Each actor is an entity (a person or an organization) that participates in a transaction or process and/or performs tasks in cloud computing. The five actors are:

- *Cloud user/cloud customer.* This is where the user accesses either paid-for or free cloud services and resources within a cloud. These users are granted system administrator privileges to the instances they start—and only those instances, as opposed to the host itself or other components.
- *Cloud provider.* This is a company that provides a cloud-based platform, infrastructure, application or storage services to other organizations and/or individuals, usually for a fee that is otherwise known to clients as "as a service."
- *Cloud auditor.* This refers to a party that can conduct independent assessments of cloud services, information system operations, performance and security of the cloud implementation.
- *Cloud carrier.* A cloud carrier is an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.
- *Cloud services broker (CSB).* The CSB is typically a third-party entity or company that looks to extend value to multiple customers of cloud-based services through relationships with multiple cloud service providers. It acts as a liaison between cloud services customers and cloud service providers, selecting the best provider for each customer and monitoring the services. A CSB provides:
    - *Service intermediation.* A CSB enhances a given service by improving some specific capability and providing value-added services to cloud consumers. The improvement can be managing access to cloud services, identity management, performance reporting, enhanced security, etc.
    - *Service aggregation.* A CSB combines and integrates multiple services into one or more new services. The broker provides data integration and ensures the secure data movement between the cloud consumer and multiple cloud providers.
    - *Service arbitrage.* Service arbitrage is similar to service aggregation except that the services being aggregated are not fixed. Service arbitrage means

a broker has the flexibility to choose services from multiple agencies. The cloud broker, for example, can use a credit-scoring service to measure and select the agency with the best score.

Cloud Deployment Models

Now that you are equipped with an understanding and appreciation of the cloud service capabilities and categories, we will look to understand how these services are merged into the relevant deployment models. The selection of a cloud deployment model will depend on any number of factors and may well be heavily influenced by an organization's risk appetite, cost, compliance, regulatory requirements, legal obligations and other internal business decisions and strategy.

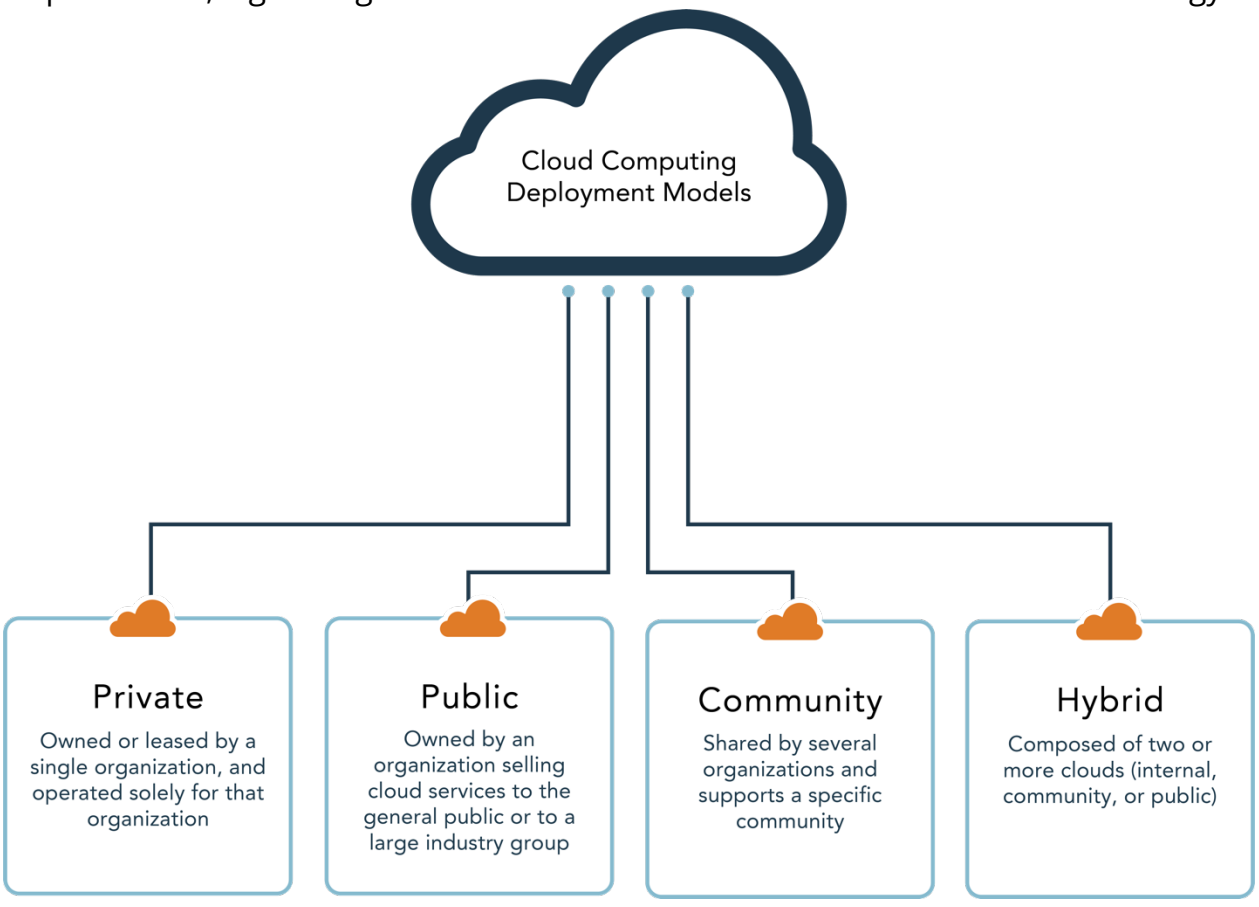


Figure 1.14: Cloud Computing Deployment Models

Private Cloud

A **private cloud** service refers to a proprietary network or data center owned and architected for use by a specific entity, utilizing cloud technologies to provide services behind a firewall. A private cloud is typically managed by the organization it serves; however, a recent increase in outsourcing the general management of this to trusted third parties has been noted. A private cloud is typically only available to the entity or organization and to its employees, contractors and selected third parties.

The private cloud is also sometimes referred to as the internal or organizational cloud. Key drivers or benefits of private cloud typically include:

- Increased control over data, underlying systems and applications
- Ownership and retention of governance controls
- Assurance over data location

Private clouds are typically more popular among large, complex organizations with legacy systems and heavily customized environments. Additionally, where a significant technology investment has been made, it may be more financially viable to utilize and incorporate these investments within a private cloud environment than to discard or retire such devices.

Virtual Private Cloud

A **virtual private cloud** (VPC) is a type of modified private cloud. While it is possible that a VPC can be implemented in a true private cloud (as defined in NIST SP 800-145 and ISO/IEC 17788), a virtual private cloud is, by definition, not a private cloud. It is implemented in the more commonly consumed public cloud, thus the term virtual. Consider that the major CSP platforms all have VPC offerings on their public cloud platforms. Virtual private clouds provide cloud consumers with the following benefits and capacities:

- Manage private IP addresses and define subnets
- Interconnect VMs to communicate across subnets
- Define access control policies for ingress and egress rules
- Implement traffic optimizers, load balancers and application firewalls

- Interconnect hybrid clouds
- Extend traditional data center reach into cloud services

The VPC is the consumer's new logical representation of the data center, but since each CSP may have different views of what constitutes a VPC, we will discuss a generalized case here. The products delivered by the CSPs include networking tools with mappings back to on-premises technologies, which guide the new cloud adopter toward familiar equivalents for their existing tools in the cloud. Increasingly, we are concerned with securing integrations between clouds, rather than migrating data centers to the cloud. The CSP-provided VPC products give the consumer the opportunity to configure subnets, network ranges, **routing tables** and **network gateways** within the VPC.

Organizations can use separate VPCs to isolate each of their organizational entities. Tiers of applications can be isolated with subnets that are designated as private or internet accessible. Organizations can decide to connect to the cloud via a virtual or physical private connection. Network access control lists can hamper performance and thus should be used sparingly for coarse-grained control. The subnet route tables for an organization's VPC should be configured with the minimal required network routes.

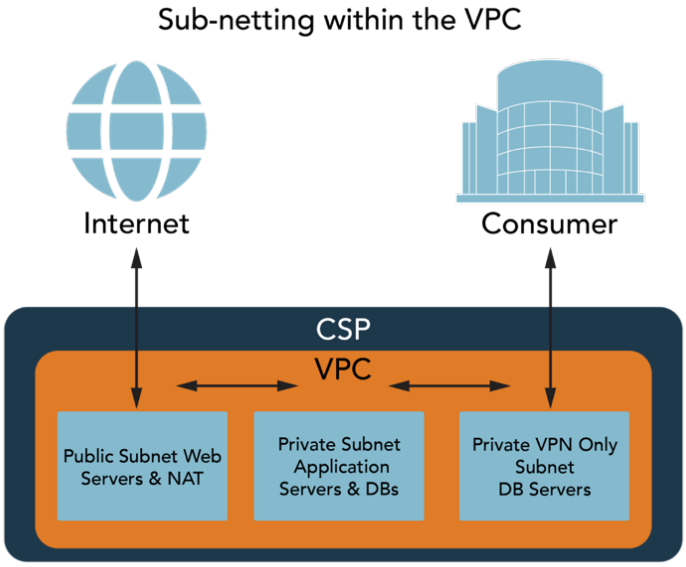


Figure 1.15: *Sub-netting within the VPC*

A subnet is configured with an IP address range. Consumers design both the public and private subnets. Network resources are provisioned by the consumer using their management console and live in a specific subnet.

Customers may add other products than those offered by the CSP, and these may deliver a common control method across multiple CSPs.

Public Cloud

A public cloud is the service available to the public over the internet in which a customer can access cloud service provider resources on demand, such as applications and storage, either as a free service or pay-per-usage. Key drivers or benefits of a public cloud typically include:

- Easy and inexpensive setup because hardware, application and bandwidth costs are covered by the provider
- Streamlined provisioning of resources
- Scalability to meet customer needs
- No wasted resources (pay per use)

Given the increasing demand for public cloud services, many providers are now offering and remodeling their services as public cloud offerings. Significant and notable providers in the public cloud space include Amazon, Microsoft, Salesforce and Google, among others.

Virtual private cloud (VPC) is not a NIST deployment model, but a description of a public cloud option where a segment of a public CSP infrastructure is segregated from the broader cloud environment for the exclusive use of a single customer. This on-demand service gives the customer a configurable pool of shared computing resources and provides a certain level of isolation from the provider's other customers. Isolation is normally achieved through allocation of private network IP subnets, a virtual local area network (VLAN), or sets of independent encrypted communication channels. Access to a customer's VPC is provided using CSP-dictated remote access procedures.

Community Cloud

Community clouds offer a valuable and cost-effective manner for specified groups or entities with a similar focus, or with common compliance and requirements, to operate in a multitenant infrastructure. Community clouds can be on premises or off site and should give the benefits of a public cloud deployment while providing heightened levels of privacy, security and regulatory compliance.

Hybrid Cloud

A **hybrid cloud** is built by combining multiple forms of cloud computing deployment models, typically public and private cloud. Hybrid cloud computing is gaining popularity, as it provides organizations the ability to retain control of their IT environments, offers the convenience of allowing organizations to use public cloud service to fulfill non-mission-critical workloads and takes advantage of flexibility, scalability and cost savings.

Key drivers of benefits of hybrid cloud deployments include:

- Retaining ownership and oversight of critical tasks and processes related to technology
- Reusing previous investments in technology within the organization
- Controlling most critical business components and systems
- Cost-effectively fulfilling noncritical business functions using public cloud components
- "Cloud bursting," defined as when a private cloud workload maximum is reached, public cloud resources are used in support, and disaster recovery can be enhanced by hybrid cloud deployments

While numerous benefits are realized with hybrid cloud deployments and cloud models, these can be time-consuming and laborious at the outset, as that's when most companies and entities encounter integration and migration issues.

Multicloud

Multicloud is a newer term not included in reference architectures that refers to using cloud services from multiple cloud service providers. While it could be

considered a special type of hybrid cloud defined by the reference architectures, it can be important to distinguish the use of services from multiple CSPs instead of a single CSP. Multicloud and hybrid are not mutually exclusive but are complementary. Many companies currently implement what could be considered a Hybrid Multicloud environment where they use public cloud services from multiple different vendors, as well as a private cloud and potentially a community cloud service.

Cloud Computing Shared Considerations

Cloud shared considerations should be coordinated and implemented consistently across an organization's cloud computing ecosystem. Responsibility for addressing these are shared issues across all actors/roles, activities and components. Also referred to as cross-cutting aspects, these items are addressed below.

Before we cover in detail the cloud computing shared considerations, we will discuss the cloud computing shared responsibility model.

Cloud Computing Shared Responsibility Model

Security of cloud data and applications is a responsibility that is shared between the cloud service provider and the cloud service consumer. One way to portray the responsibility boundary is:

- The CSP has responsibility for security *of* the cloud.
- The customer has responsibility for security *in* the cloud.

Of-the-cloud security describes the task of protecting the cloud infrastructure. This includes both the physical and logical protection of hardware, software, networking and facilities that run cloud services.

In-the-cloud security responsibilities are dictated by the specific cloud services consumed by customers. Those responsibilities include service configuration and management tasks, management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on compute instances, and the configuration of the ACSP-provided firewalls on each instance.

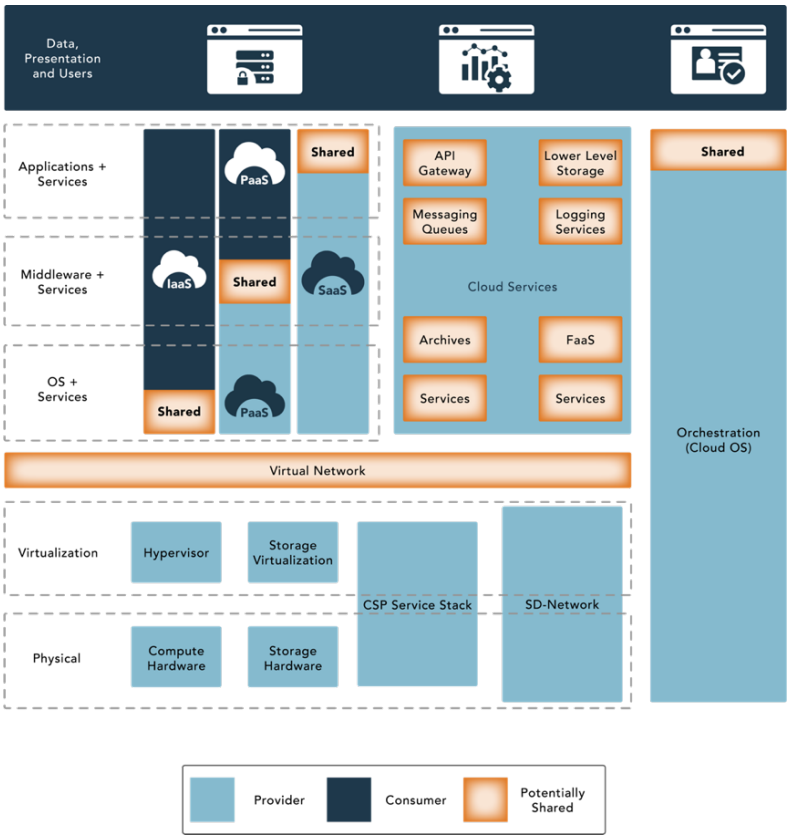


Figure 1.16: Shared Security Model

The cloud computing shared considerations will now be explored in more detail.

Auditability

Auditability relies on a single key component: evidence. Think of the auditor coming in with their checklist and questions today—that is the same mindset an organization should take to ensure that it always has a comfort with, and positive understanding of, its ability to audit and measure actions against requirements. Systems and processes will fail, so wherever possible, auditing and auditability should provide enough information, details and evidence to support reviews and investigations. The ability to point to audit results, findings and relevant evidence has not only saved jobs and companies from catastrophic impacts, but also has given leaders the facts and reports they need to alter business processes, system functions and personnel activities and to implement increased safeguards such as defense in depth or additional layers of security and risk management.

Availability

Systems and resource availability define the success or failure of a cloud-based service. Availability is a single point of failure for cloud-based services. If the service or cloud deployment loses availability, the customer is unable to access its target assets or resources, resulting in downtime. In many cases, cloud providers are required to provide upwards of approximately 99% availability as per the service-level agreement. Failure to do so can result in penalties, reimbursement of fees, loss of customers, loss of confidence and, ultimately, brand and reputational damage.

Compliance

Regulatory compliance is an organization's requirement to adhere to laws, regulations, guidelines and specifications relevant to its business, specifically dictated by the nature of operations and functions it provides to its customers. Where the organization violates or fails to meet regulatory compliance regulations, punishment can include legal actions, fines and potentially halting business operations or practices. Key areas that are often applicable to cloud-based environments include (but are not limited to) the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA) and the Sarbanes-Oxley Act (SOX).

Governance

The term governance, when relating to processes and decisions, refers to defining actions, assigning responsibilities and verifying performance. The same can be said and adopted for cloud services and environments where the goal is to secure applications and data when in transit and at rest. In many cases, cloud governance is an extension of existing organizational or traditional business process governance, with a slightly altered risk and controls landscape. While governance is required from the commencement of a cloud strategy or **cloud migration** roadmap, it is seen as a recurring activity and should be performed on an ongoing basis. A key benefit of many cloud-based services is the ability to access relevant reporting, metrics and up-to-date statistics related to usage, actions, activities, downtime, outages or updates. This may enhance and streamline the governance

and oversight activities with the addition of scheduled and automated reporting available.

Processes, procedures and activities may require revision after migration or movement to a cloud-based environment. Not all processes remain the same. Segregation of duties, reporting and incident management are examples of processes that may require revision after cloud migration.

Interoperability

Interoperability is the requirement for the components of cloud ecosystems to work together to achieve their intended result. In a cloud computing ecosystem, the components may come from various sources that are both cloud and traditional and from both public and private cloud implementations known as hybrid cloud. Interoperability mandates that these components should be replaceable by new or different components from different providers and continue to work, as should the exchange of data between systems. If a car engine fails, for example, the owner should be able to replace the engine with the same brand or type of engine, or alternatively look for another engine that will provide the same level of power and function to allow the car to operate. Interoperability uses the same premise—continued availability of services, regardless of providers or cloud components.

Maintenance and Versioning

Maintenance refers to changes to a cloud service or the resources it uses to fix faults, upgrade or extend capabilities for business reasons. Versioning implies the appropriate labeling of a service so that it is clear to the cloud service customer that a particular version is in use.

Performance

Cloud computing and high performance should always go hand in hand. If the performance is poor, a customer may not be a customer for long. For the best experience using cloud services, provisioning, elasticity and other associated components should always focus on performance. The speed at which a boat travels is dependent on the engine and the boat design. The same applies to performance, which should always be focused on the network, compute, storage and data. With these four elements influencing the design, integration and

development activities, performance should be boosted and enhanced throughout. Remember, it is always harder to refine and amend performance once design and development have been completed.

Portability

Portability defines the ease with which application components are moved and reused elsewhere regardless of the provider, platform, OS, infrastructure, location, storage, format of data or APIs. Portability is a key aspect to consider when selecting cloud providers, since it can both prevent vendor lock-in and deliver business benefits by allowing identical cloud deployments to occur in different cloud provider solutions, either for the purposes of disaster recovery or for the global deployment of a distributed single solution. Again, think of car components. Light bulbs, brakes and other standard components could be switched out, yet the car would continue to function.

Privacy

In the world of cloud computing, privacy presents a major challenge for customers and providers alike. No uniform or international privacy directives, laws, regulations or controls exist, leading to a separate, disparate and segmented mesh of laws and regulations being applicable, depending on the geographic location where the information may reside (data at rest) or be transmitted (data in transit). Given the true global nature and various international locations of cloud-computing data centers, this could mean that an organization's data could reside in two, three or more locations around the world at any given time. For many entities and organizations operating in Europe, this violates European Union (EU) data protection laws and obligations, which could lead to various issues and implications.

Regulatory

Many different regulations influence the use and delivery of cloud services. Statutory, regulatory and legal requirements vary by market sector and jurisdiction, and they can change the responsibilities of both cloud service customers and cloud service providers. Compliance with such requirements is often related to governance and risk management activities.

Resiliency

Cloud resiliency represents the ability of a cloud services data center and its associated components—including servers and storage, for example—to continue operating in the event of a disruption, which may be caused by equipment failure, power outage or natural disaster. Since most cloud providers have a significantly higher number of devices and redundancies in place than a standard in-house IT team, cloud resiliency should typically be far higher, with equipment and capabilities ready to failover, multiple layers of redundancy and enhanced exercises to test such capabilities.

Reversibility

Reversibility is a process for the cloud service customer to retrieve its cloud service customer data and application artefacts and for the cloud service provider to delete all cloud service customer data and contractually specified cloud service derived data after an agreed period.

Security

For many customers and potential cloud users, security remains the single biggest concern, with as much as 60% of business users stating that security concerns are the number one restriction or barrier preventing them from engaging with cloud services. As with any successful security program, the ability to measure, obtain assurance and integrate contractual obligations to minimum levels of security are key. Many cloud providers now list their typical or minimum levels of security but will not list or state specific security controls for fear of their infrastructures being targeted by attack vectors and threats. When contracts and engagements require specific security controls and techniques to be applied, these are typically seen as extras that incur additional costs and require the relevant nondisclosure agreements (NDAs) to be completed before engaging in active discussions.

For smaller organizations, a move to cloud-based services will significantly enhance security controls, given that they may not have access to, or possess the relevant security capabilities of, a large-scale cloud-computing provider. The rule of thumb for security controls and requirements in cloud-based environments is that more

security equals added costs. Customers can have whatever they want when it comes to cloud security, as long as they are willing to pay for it.

Service Levels and Service-Level Agreements (SLAs)

The cloud computing service-level agreement (cloud SLA) is an agreement between a cloud service provider and a cloud service customer based on a taxonomy of cloud computing-specific terms to set the quality of the cloud services delivered. It characterizes quality of cloud services delivered in terms of measurable properties specific to cloud computing (business and technical) and a given set of **cloud computing roles** (cloud service customer, cloud service provider and related sub-roles).

Outsourcing

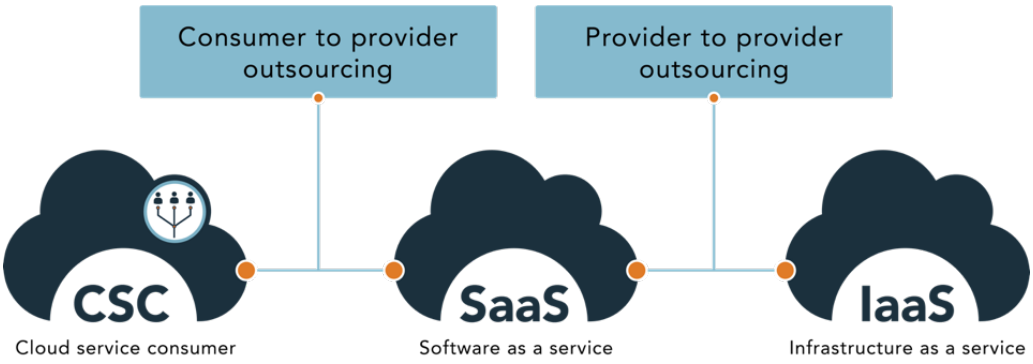


Figure 1.17: Outsourcing

Cloud consumers may outsource some functions to external providers, which may include cloud service providers or those that use a cloud service for their functions. Cloud service providers at the SaaS or PaaS levels may also run their services atop an IaaS provided by another CSP. This can create a multilayer supply chain scenario where cloud services are used to support various business functions and have data resident within them that are not directly contracted from the originating organization.

It is important for consumers to understand the supply chain for any service so potential cloud-related issues can be identified. This can be particularly important for sensitive data or regulated data types.

Since SaaS providers may rely on other PaaS or IaaS providers, and PaaS providers may rely on other IaaS providers, understanding the underlying business relationships in any supply chain or outsourcing arrangement will help to identify potential risks in a multitier environment. For instance, if a SaaS provider that is being relied upon for business services from cloud consumers changes IaaS providers or is involuntarily deplatformed by an IaaS provider, this can significantly impact all the SaaS provider customers. Similar issues may arise from geographic locations or legal jurisdictions of underlying providers that may not be obvious to the service consumer. Understanding where such outsourcing agreements may exist with cloud services is an important consideration for developing a realistic risk model.

Impact of Related Technologies

NIST defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. NIST implies the economy of scale that goes with cloud computing when addressing a pool of configurable computing resources.

Cloud computing provides the foundational information technology services for many of the most desirable business-related capabilities including:

- Data Science
- Machine Learning
- Artificial Intelligence
- Blockchain
- Internet of Things (IoT)
- Containers
- Quantum Computing
- Edge Computing
- Confidential Computing

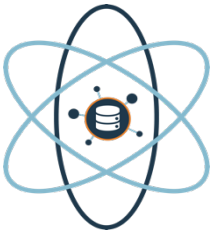
These capabilities are made economically viable by the automation, elasticity and scalability of cloud computing infrastructures. In addition, each of these capabilities also makes new and valuable business models viable.

Blockchain, for instance, enables global visibility of a shared transaction accounting ledger. Initially used to establish and manage cryptocurrencies, important business value can be delivered by inherent capabilities that include:

- Increased security because of its decentralized nature, which means that data is stored on thousands of different servers with no central point of failure
- Proof of work consensus that can verify each transaction across all the nodes using hashing algorithms to authenticate and validate transactions
- Creation of an immutable ledger, which means that alteration or falsification of data is impossible without every participant knowing of its occurrence
- The use of time-stamped transaction verification across the entire ledger, which allows for real-time data and elimination of fraud
- The ability to use fractional ownership and tokenization of assets

Both machine learning and artificial intelligence (AI) previously required large capital expenditures on specialized computer hardware and software. This made business use of these types of services unaffordable for all except the highest-margin business models. The use of commodity infrastructure, scalable compute services and on-demand pricing lowers the cost to a level that is now affordable for most business models. IoT solutions are now made economically viable by the low cost and widespread availability of cloud-based machine learning and artificial intelligence services.

Data Science



Data science is the analysis of data in different forms to draw insights or develop useful information from it. With the emergence of cloud-based technologies, data is stored, accessed and manipulated in novel ways, which has required new techniques to identify and analyze data. This is especially true with the ever-increasing size of data sets made possible by the cloud. Terms

such as big data and data lakes have been coined to represent application of data science techniques to increasingly large and diverse data sets to extract useful insights or actionable information from the data sets.

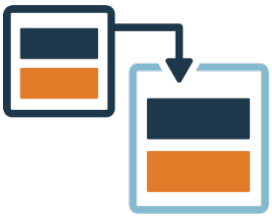
Artificial Intelligence and Machine Learning

AI and machine learning (ML) are closely related topics. AI is a general term for any technology or set of technologies that emulates human behavior or interactions. AI has had many definitions applied to it over the years and is often used more as a marketing term than a meaningful representation of what a service or capability provides; it can be applied to any type of intelligent machine or service.

ML, often considered a branch of AI science, is a method used to create intelligent products or services. ML trains automated systems by using computer programs to adjust algorithms that produce desired results quickly and efficiently. In many cases, this can create better and faster results than a human attempting to manually code or adjust the algorithms.

Both AI and ML benefit from the resources available in the cloud but are also extremely useful tools to apply to the vast data sets available in the cloud. Cloud resources can be used to support the processor-intensive training required for ML in support of AI functions, but AI in its many forms can perform advanced analyses of cloud-based data sets that would otherwise be impractical to undertake.

Blockchain



Blockchain technologies make cryptographically secured transaction registers or ledgers that contain built-in integrity protections. Blockchain technology can be used in any circumstance that needs an integrity-protected transaction register. It is often used to secure distributed transaction records that involve numerous independent nodes such as cryptocurrency systems. Blockchain is separate from cryptocurrency systems, but it is often used within those systems to protect the integrity of transactions.

Blockchain solutions may be suitable for systems that require:

- Many participants
- Distributed participants
- The ability to operate without a trusted third party
- Workflow that is transactional in nature (e.g., the transfer of digital assets/information between parties)
- A globally scarce digital identifier (i.e., digital art, digital land, digital property)
- A decentralized naming service or ordered registry
- A cryptographically secure system of ownership
- The ability to reduce or eliminate manual efforts of reconciliation and dispute resolutions
- The ability to enable real-time monitoring of activity between regulators and regulated entities
- Full provenance of digital assets and a full transactional history to be shared among participants

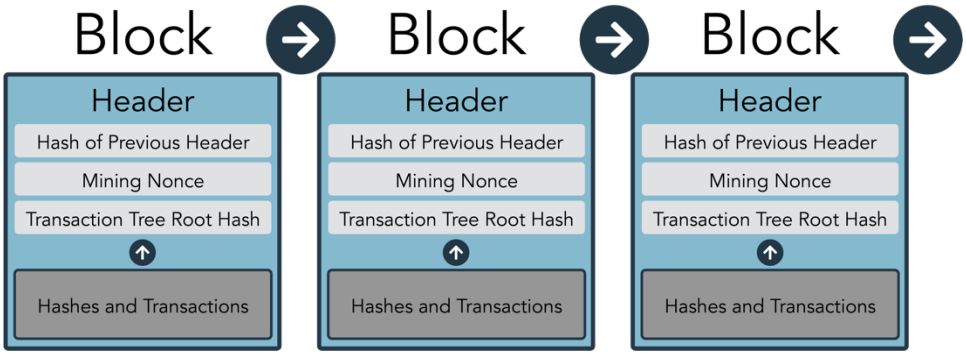
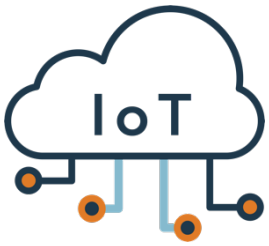


Figure 1.18: Blockchain built with Cryptographic Hash Functions

Internet of Things (IoT)

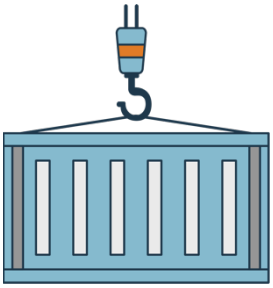


IoT is a generic term for numerous products that include physical objects with embedded sensors, controls that interact with upstream controllers or other IoT devices.

By nature, IoT is highly distributed, but also highly connected. IoT often must interact with upstream controllers or other IoT devices. IoT devices also tend to be small-form factor, low-power appliances, or devices with limited onboard computing capabilities. All of this makes integration with the cloud a huge benefit for many IoT capabilities.

Current and emergent cloud services can help manage IoT deployments, provide inventories and update IoT devices. Some services can act as central communication platforms between other applications and IoT devices or between IoT devices. In other cases, cloud services can supplement limited onboard capabilities of IoT devices by supporting AI or ML functions for IoT or providing back-end processing for IoT (e.g., voice assistants that offload natural language processing to a cloud service).

Containers



Containers are software packages that contain all necessary code, including libraries and dependencies, needed to run that package. Containers are not full virtual machines and do not contain operating system functions beyond what the software package needs to run.

Containers can be implemented in a variety of ways—for example, Linux containers, the capability for which is built into the operating system itself. In other cases, dedicated container platforms can be deployed that can run many containers.

Containers are more lightweight than the full virtualized operating system found in a traditional VM, and they use fewer resources. This also makes them faster to start or stop.

Deployment of containerized applications has become a common feature of the cloud and can be used to support the concept of cloud elasticity by allowing rapid expansion of deployed instances (copies of containers) that can be rapidly reduced when no longer necessary.

Quantum Computing

Quantum computing is an emerging computing architecture that uses quantum states and qubits to perform calculations. While normal binary digits are either a 0 or 1, a qubit can effectively be a 0, 1 or in a superposition of both states. Current quantum computers are limited, but emerging cloud services from various providers allow access to the limited quantum computing systems available. Quantum computing has the potential to solve historically difficult calculations at a much lower computational cost. This has several potential use cases, but current practical implementations are limited.

There is some concern of the potential for quantum computing systems to more efficiently solve certain mathematical problems used in traditional cryptographic mechanisms, which could result in some cryptographic algorithms becoming weaker than is currently the case. This primarily involves the specific algorithms that use factoring or large prime numbers. The degree to which quantum computers could degrade cryptography based on these algorithms is not yet fully understood, but many of the affected algorithms are already considered deprecated and have been transitioning out of most use cases for several years. However, some—such as the RSA algorithm for public key cryptography—are still in common use for internet security applications. Transition away from these legacy algorithms may become imperative once quantum computing becomes widely available.

Edge Computing

Edge computing is a general term for any of several technologies that bring computing elements (e.g., computer, storage) closer to data sources or service requesters. The main goal is to reduce latency in transactions or requests. The term fog computing may be applied synonymously with edge computing. Some IoT implementations may be considered a type of edge computing, but other implementations may exist transparently to service requestors or system users. For example, a Content Distribution Network (CDN) is a technical implementation of edge computing concepts where high bandwidth content (e.g., images, files) is distributed to edge computers located worldwide, so that when content is requested for a web page (e.g., a large image) that content can be delivered quickly from the closest edge server. The CDN uses backend services to distribute and synchronize the content among all edge servers.

Edge computing is used in many cloud-based services and infrastructures to support high bandwidth and low latency requirements across geographically dispersed areas.

Confidential Computing

Confidential computing is a computing technology that isolates sensitive data in a protected CPU enclave during processing. This has been traditionally difficult to do in the cloud, as opposed to protections for data at rest or in transit and relies on hardware support to enable. Confidential computing is still an emerging technology for the cloud, and architectures require the adoption of hardware platforms that support hardware-level trusted execution. Using appropriate hardware and software components, a confidential computing environment can be built by the CSP that retains data in memory in an encrypted form and only decrypts data as it moves from memory to the processor. The secure/protected hardware enclave that supports this may be referred to by different names but is often generically described as a Trusted Execution Environment (TEE). Different hardware architectures have differing technical implementations for a TEE and may use

different vendor-specific names, but they all provide some level of hardware-based assurance that information will be protected for confidentiality and integrity while it is resident within the TEE.

The use of confidential computing technologies or services enhances data isolation from the CSP and CSP operated hardware components. This provides some protection of data from the CSP as well as potential data compromise if another tenant accesses the memory of the underlying cloud infrastructure.

Cloud Economics

Cloud computing is often referred to as a technology. However, it is actually a paradigm shift in the business and economic models for provisioning and consuming information technology that can lead to significant cost savings. This cost savings can only be realized through using significant pooling of these "configurable computing resources" or resource pooling. This capability is an essential characteristic of cloud computing. Resource pooling defines the ability of a cloud to serve multiple consumers using a multitenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Economic Impact of the Cloud Computing Model

Businesses must deal with the disparity between producing products and delivering services—which is fixed in the short term—and the demand for those products and services—which can be variable on any time scale. Customer demand can be volatile. While tactical measures can be taken to alleviate some scenarios, cloud computing models are capable of economically solving the demand dilemma when applied to cloud computing-compatible business models.

Cloud computing can economically address the capacity conundrum, when companies build capacity to match peak demand, which typically leads to substantial excess capacity during off-peak periods. This excess capacity represents either nonproductive capital or unnecessary expense. Conversely, if capacity is sized to the baseline, there will be insufficient resources to handle spikes. Transactions not served represent demand for the products or services that the

business would have monetized, resulting in lost revenue or lost worker productivity.

For the cloud service provider, cloud computing economics depends on the expected consumption characteristics of the targeted customer population. These factors drive the cloud provider's ability to use the minimum amount of physical IT resources to service a maximum level of IT resource demand. Balancing these factors across a well-characterized user group can lead to an approximate 30% savings in IT resources. This enables the near-real-time modification of the underlying physical infrastructure required for the delivery of an illusion of infinite resources that is part of cloud-computing users' experience.

Cloud service providers bring massive economies of scale to computing and deliver computing resources on demand. Before cloud computing, companies had to make ever-growing capital expenditures in computing resources to implement new information systems and to accommodate potential peak loads. This led to overcapacity and underutilization. Cloud computing can help exploit short-term business opportunities, because cloud computing services are consumed using a variable OpEx model, which:

- Eliminates long-term investments when exploring new business models.
- Is an efficient enabler of cross-device access and synchronization of content or applications across a single user with multiple devices.
- Eliminates hardware costs normally associated with new systems or services.

This combination drives the information technology industry away from highly customized independent architectures that drive prevailing prices upward. Cloud computing drives the industry towards pooled resources, shared architectures, flat-rate pricing models and pay-per-use pricing models that lower prevailing prices.

A 2009 Booz Allen Hamilton study concluded that a cloud computing approach could save 50-67% of the life cycle cost for a 1,000-server deployment. A separate Deloitte study confirmed that cloud computing deployments delivered greater investment returns with a shorter payback period when compared to the traditional on-premises option. These studies show that, when implemented

properly, the IT service delivery model can drastically reduce the operations and maintenance cost of IT infrastructures. Verification of these findings by many other independent studies, along with the rapid proliferation of billion-dollar, born-in-the-cloud startups, accelerated the continuing and broad-based rapid growth and adoption of the cloud computing economic model.

The figure below shows a generic project cost curve with the rate of project expenditure over time. This model can be applied to help understand the expected costs of moving a service to the cloud. The goal is to minimize upfront expenditures during a transition period with the expectation that the long-term expenditure rate will significantly decrease from existing costs. The final return on investment will be dependent on how much new ongoing costs are reduced below existing ones, as well as the length and magnitude of expenditures during the transition phase. A common error is to base cloud transition solely on the difference between the existing and new ongoing service costs, without consideration of the transition costs, as well as the risk that the new ongoing costs will not end up being as low as projected.

Depending on the specifics of what is being transitioned, the transition costs could include new development, acquisition of new or upgraded software and configuration of cloud services, all in parallel with the existing service that will drive overall expenditures above existing costs for some period. As the old service is decommissioned, ongoing expenditures should drop to a new steady state, which is hopefully much lower than before. With cloud transitions, a common risk is with delays in decommissioning existing services, which draws out the timeline for the transition period, and in some cases, the existing service may not be fully decommissioned for a lengthy period.

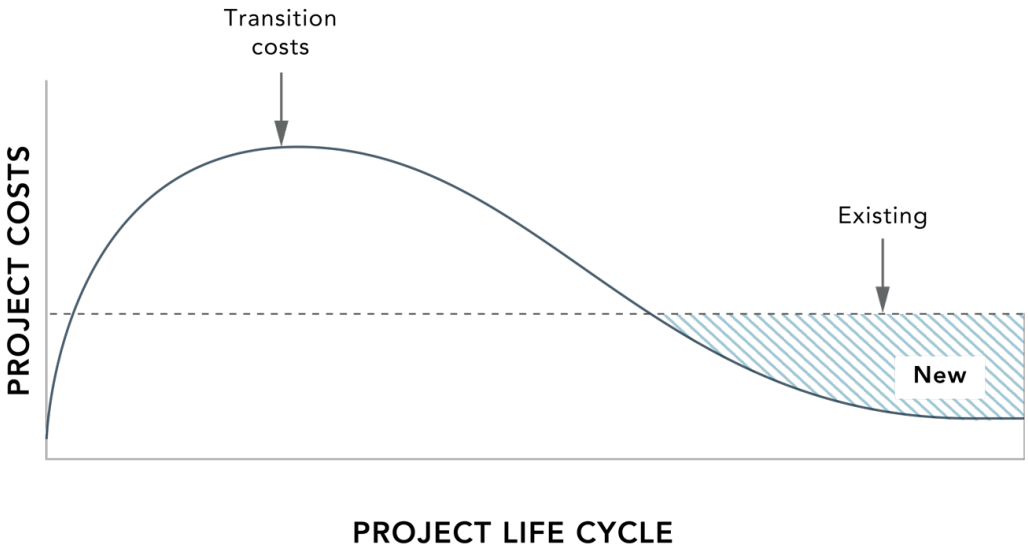


Figure 1.19: Cloud Deployment Economic Model

Traditional vs. Cloud Model

As noted above, changes in demand must be matched by changes in capacity. Figure 1.20 shows the different responses of a traditional model and the on-demand model offered by the cloud. In the traditional model, it is necessary to plan for capacity requirements while often exceeding the expected demand to handle spikes. This results in wasted capacity most of the time and can result in failure if demand exceeds capacity.

In the on-demand model offered by most cloud services, capacity allocated to the service closely follows actual demand, resulting in minimum wasted capacity at the service or application level while still supporting unexpected demands.

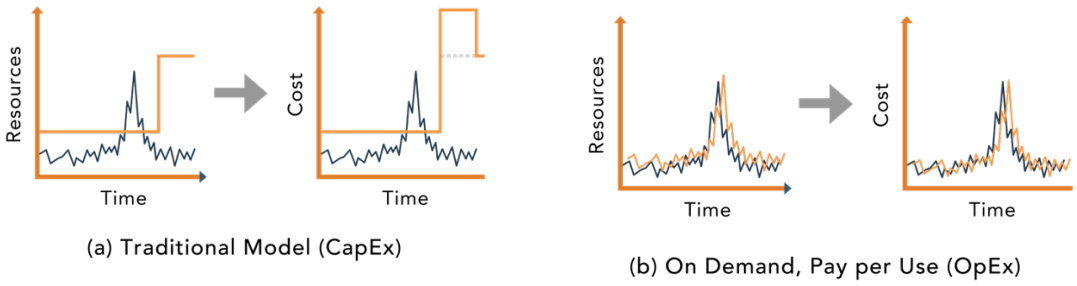


Figure 1.20: Cloud Computing Versus Traditional IT Economic Model

Cloud Transition Economics

Transitioning from a traditional enterprise IT infrastructure to the cloud model involves a significant level of investment, operational modification and cultural change. Investment is driven by an increased use of automation, staff skillset enhancements and training costs associated with needed operational changes.

Operational modifications are associated mostly with "brutal" enforcement of standards across the organization. Aggressive enforcement of standards is essential to the broad and deep deployment of automation needed to effect significant staff reductions and effective service-level management.

The significant cultural changes associated with the operational modifications should not be underestimated. Cultural changes will permeate the entire organization for five or more years if done across a global organization. Research has also shown that the cost of private cloud deployments may exceed the operating cost of an established traditional operation. Organizations should also be cautioned about the relative rarity of cost savings associated with a transition to a private cloud. Cost savings are much more likely if a subset of requirements is addressed through a private cloud and the balance appropriately met with the adoption of public or community cloud services. Resulting hybrid cloud models have been shown to significantly reduce operating costs while simultaneously improving operational efficiency.

Public Cloud Adoption Economics

While all cloud types offer potential economic benefits, public cloud adoption has historically delivered significant enterprise IT cost savings through significantly reduced capital expenditures, staff level reductions and increased operational efficiencies. These well-documented results are driven primarily by public cloud service providers' ability to deliver a continuously improving level of service at lower cost and higher profit margins. Consistency in these trends is reinforced by global scale, extremely low marginal cost to deliver services to additional customers and steadily improving CSP operational efficiencies.

Understand Security Concepts Relevant to Cloud Computing (1.3)

Objective

- Summarize cloud computing security concepts.

Overview

This section introduces several general security concepts relevant to cloud computing. The security concepts are not unique to cloud computing, and in some cases may be implemented within cloud computing environments in nearly the same fashion as in traditional environments. In other cases, a new approach to implement these concepts may be necessary for the cloud environment.

For some cloud services, the security concepts may be integrated into the service itself (e.g., a SaaS may use an integrated Identity and Access Management capability) or completely transparent to the cloud consumer (e.g., hypervisor security). In any case, it is necessary to understand how the shared security model between cloud provider and cloud consumer is implemented for any given cloud service so that the consumer can choose the cloud vendor that best meets their needs but also to ensure that the consumer understands and implements consumer responsibilities.

Cloud computing security must always address: The CIA Triad

Figure 1.21: CIA Triad

Confidentiality

More than 2,000 years ago, Hippocrates, a Greek physician, first voiced the idea that a legitimate need exists for some things to be kept confidential. His patients, he said, deserved to have their medical information held private. Today, confidentiality is interpreted as stopping the unauthorized disclosure of information to someone who does not have a valid need to know, as it can potentially harm the owner or holder. This harm can be direct or indirect and usually is related to a loss of competitive or other legitimate advantage. Businesses have a legitimate need to keep private accounting and financial records such as bank statements, payroll records, supplier agreements and information about their customers. Need to know is usually understood as the person or organization in question having a lawful task, duty or purpose to learn or make use of data and the meaning inherent in the information.

Integrity

Information must be complete and correct in all relevant details to be used in making decisions and taking actions. This requires that data be kept free from unauthorized modifications throughout the life of that data in the organization's use or possession. Data integrity goes directly to its trustworthiness: If the data shown on an organization's computer systems cannot be trusted, that data is useless. It cannot be assumed that the data is correct; it must be ensured by using both technical controls and auditing tools.

Availability

Data is available when it is needed, where it is needed and in the form that is needed for it to be meaningful and useful in making decisions and taking actions. If data is kept confidential and the data is genuine, but it cannot be accessed when needed, it is useless. Companies spend significant amounts of money to ensure that their data is available to them when they need it. For example, ransomware is a growing concern affecting data availability. In some cases, backup restoration takes too long for the company to endure; it resolves to pay the ransom to resume operations in a timely manner, taking a gamble that the attacker will release data, free from encryption.

Governance, Risk Management and Compliance (GRC)

An approach commonly known as governance, risk management and compliance (GRC) has evolved to analyze risks and manage mitigation in alignment with business and compliance objectives. Governance ensures the business focuses on core activities, clarifies who in the organization has the authority to make decisions, determines accountability for actions and responsibility for outcomes and addresses how expected performance will be evaluated. All of this happens within a clearly defined context that might span a division, the entire organization or a specific set of cross-discipline functions.

Design of the governance process should be done after the organization has:

- Identified its desired outcomes.
- Identified the organizational role responsible for attaining each outcome.
- Identified the relevant metric(s) that indicate attainment of each goal.
- Outlined the decision-making process for each goal.

Risk management is a systematic process for identifying, analyzing, evaluating, remediating and monitoring risk, as well as transferring risk to another party, avoiding the risk altogether or assuming the risk with its potential consequences. Risk management should be a component of any adopted decision-making process. As a result of the risk management process, an organization or group might decide to mitigate a risk, transfer it to another party or assume the risk along with its potential consequences.

Compliance refers to actions that ensure behavior that complies with established rules as well as the provision of tools to verify that compliance. It encompasses compliance with laws as well as the enterprise's own policies, which in turn can be based on best practices. Compliance requirements are not static, nor are they geographically homogenous. This means effective compliance efforts must be both dynamic and adaptable to local or regional requirements. In cloud computing, this is especially critical when dealing with data protection and privacy.

Cryptography and Key Management

Cryptography is a method of disguising information in the presence of adversaries. Cryptography is an important tool for providing services such as confidentiality, integrity, authenticity (proof of origin), non-repudiation and access control.

Using cryptography to protect data is referred to as **encryption** and describes the process of converting plain text (readable data) into cipher text (unreadable data) to prevent unauthorized access. When data is encrypted, the only way to decrypt the data is with the corresponding **cryptographic key**.

Key management is the structure for overseeing the creation, issuance, revocation, recovery, distribution and destruction of cryptographic keys. Key management is highly important to any organization utilizing cryptography for secure communications and data protection.

More about cryptography and key management is included in Domain 2.3.

Control Frameworks

To meet security and privacy requirements, many organizations adopt control frameworks to provide a governance program that is:

- *Consistent.* An IT governance program must be consistent with enterprise executive guidance and expectations regarding organizational information security and data privacy protection goals.
- *Measurable.* The governance program must provide a way to determine progress and set goals. Most control frameworks contain an assessment standard or procedure to determine compliance and, in some cases, risk as well.
- *Standardized.* A control framework should rely on standardizations or results from one organization or part of an organization that can be compared in a meaningful way.
- *Comprehensive.* The selected framework should cover the minimum legal and regulatory requirements of an organization and be extensible to accommodate additional organization-specific requirements.

- *Modular.* A modular framework is more likely to withstand the changes of an organization because only the controls or requirements needing modification are reviewed and updated.

Useful references for establishing appropriate control frameworks include Governance of Information Security (ISO 27014: 2020) and Governance of Information Technology (ISO 38501:2015).

Enterprise Security Controls

The essence of IT governance is in the selection and application of security controls that protect organizational data while simultaneously minimizing operational friction or disruption. The continuum of security controls extends over three classes or categories:

- *Management (administrative) controls.* Policies, standards, processes, procedures and guidelines set by corporate administrative entities (e.g., executive- and/or mid-level management).
- *Operational and physical controls.* Operational security (execution of policies, standards and processes, education and awareness) and physical security (facility or infrastructure protection).
- *Technical (logical) controls.* Access controls, identification and authentication, authorization, confidentiality, integrity, availability and non-repudiation.

They also encompass the following types:

- *Directive controls.* Often called administrative controls, these are intended to advise employees of the behavior expected of them during their interfaces with or use of the organization's information systems.
- *Preventive controls.* Included in preventive controls are physical, administrative and technical measures intended to preclude actions violating policy or increasing risk to system resources.
- *Deterrent controls.* Deterrent controls involve the use of warnings of consequences to security violations.

- *Compensating control.* Also called alternative control, this is a mechanism put in place to satisfy the requirement for a security measure deemed too difficult or impractical to implement at the present time.
- *Detective controls.* Detective controls involve the use of practices, processes and tools that identify and react to security violations.
- *Corrective controls.* Corrective controls involve physical, administrative and technical measures designed to react to the detection of an incident to reduce or eliminate the opportunity for the unwanted event to recur.
- *Recovery controls.* Once an incident occurs that results in the compromise of integrity or availability, the implementation of recovery controls is necessary to restore the system or operation to a normal operating state.

It should be noted that control classes can vary based on the context of the security environment. In certain organizations, the control classes might be known as administrative, physical and technical. HIPAA, for example, defines control classes as administrative, physical and technical, but federal agencies represent them as management, operational and technical. The appropriate use of a control class, therefore, depends on the context of the organization and the regulatory and compliance management aspects that govern the organization.

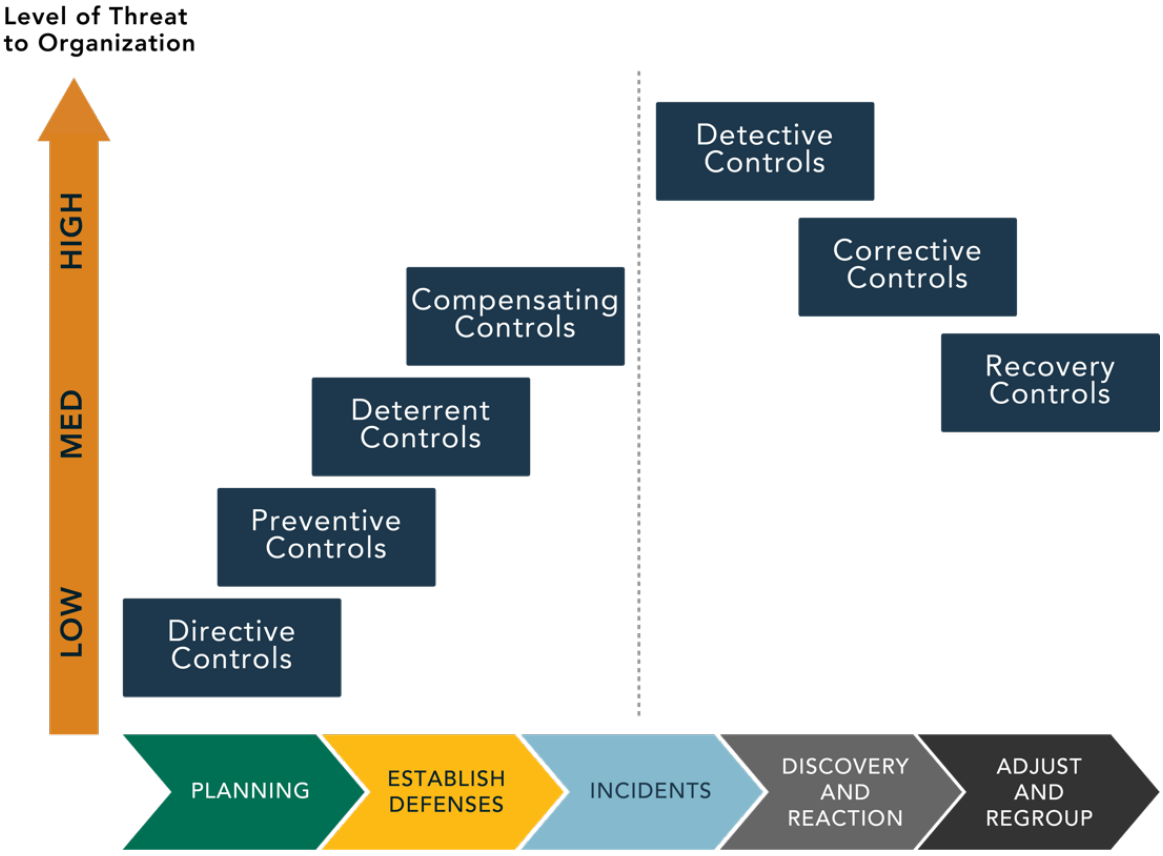


Figure 1.22: Continuum of Controls Relative to the Timeline of a Security Incident

Identity and Access Control

Identity and Access Management (IAM, sometimes IdAM) is a broad category that covers:

- *Identity provisioning and deprovisioning.* Digital identities are created and issued to the identity owner with some degree of identity proofing, and when no longer needed, digital identities are removed.
- *Authorization,* which can include:
  - *Management function.* Organizational decision process to determine the users or digital identities who should be granted privileges to data. At this level, authorization is typically governed by an organizational process for determining appropriate access that is used to grant or revoke access to specific resources.

  - *Per access attempt.* The process of verifying that a requested action or service is approved for a specific entity. At this level, an access request will be evaluated to determine whether an entity requesting access is authorized to do so based on configurations derived from the authorization management process. Normally, this is the technical component of **authorization**.
  - *Granting and revoking access privileges (process).* Access control mechanisms are configured to permit authorized activities and access. When no longer needed, obsolete access privileges are removed or downgraded. Granting and revoking access privileges is a governance process that ensures proper access controls are configured on systems and services.
  - *Identification.* Claim of an identity by a subject (e.g., presentation of a username by a user).
- *Authentication.* Process that requests one or more factors of authentication—for example, a password— to validate that the identity claimed by a user or entity is known to the system. Factors typically include something that the user is (i.e., a fingerprint), something they have (i.e., a hardware security token) and something they know (answers to challenge questions). Single factor (SFA) authentication verifies with only one of these; multifactor (MFA) uses two or more.
  - *Allow/Deny Access (per access attempt).* Access is granted or denied for each access request made by a system entity or user to any resource based on the authorization for that entity or user.
  - *Accounting.* Access control process which records information about all attempts by all identities to access any resources of the system.

The below diagram shows a general depiction of the identity life cycle.

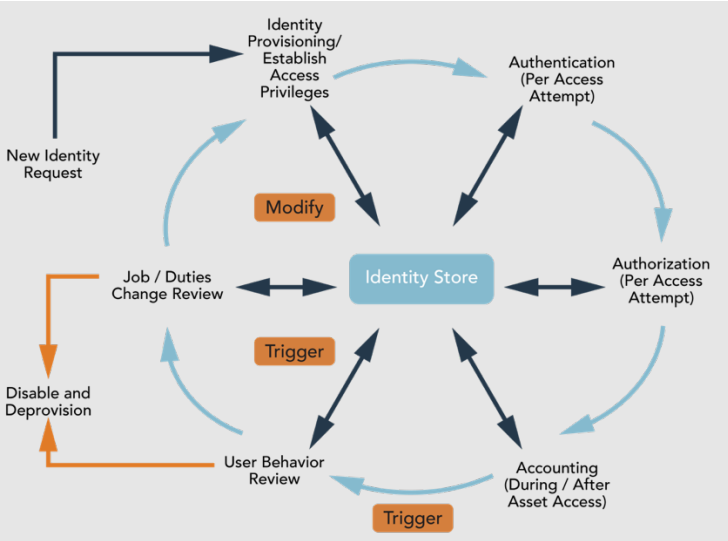


Figure 1.23: The Identity Life Cycle

Authorization and Access Management

The traditional data life cycle model does not specify requirements for who can access relevant data, nor through which devices and channels they can access it. Access to devices, systems and resources forms a key driver for the use of cloud services. Many cloud services may integrate identity, authorization and access management capabilities that already exist in traditional networks or allow federation with other cloud service capabilities. Cloud services, especially at the SaaS level, may also extend traditional access control, which has often been focused on who can access what from where, using which device or communication channel. This can obviously add complexity and require new or revised policies and procedures. However, it can also produce a much more granular access control system overall.

In the same way that users require authorization and access management to be operating and functioning to access the required resources, security also requires these service components to be functional, operational and trusted to enforce security within cloud environments.

In its simplest form, authorization determines the user's right to access a certain resource (think of entry onto a plane with a reserved seat or visiting an official residence or government agency to visit a specified person). In a broader context, authorization can include the processes and human decisions that go into determining whether an entity should be granted access. However, technical components also conduct authorization, using various forms of access control that determine whether access should be granted based on roles, rules or some form of logic based on attributes.

Note that both authorization and access management are "point-in-time activities" that rely on the accuracy and ongoing availability of resources and functioning processes, segregation of duties, privileged user management, password management, etc., to operate and provide the desired levels of security. If any of the activities mentioned are not carried out regularly as part of an ongoing managed process, this can weaken the overall security posture.

Provisioning and Deprovisioning

Provisioning and deprovisioning are critical aspects of access management—think of setting up and removing users. In the same way that an account would be set up for a user entering an organization who requires access to resources, provisioning is the process of creating accounts to allow users to access appropriate systems and resources within the cloud environment.

The goal of user provisioning is to standardize, streamline and create an efficient account creation process, while creating a consistent, measurable, traceable and auditable framework for providing access to end users.

Deprovisioning is the process whereby a user account is disabled when the user no longer requires access to the cloud-based services and resources. This is not just limited to a user leaving the organization but may also be due to a user changing role, function or department. Deprovisioning access that is no longer required may involve removing permissions or technical access rights on systems. Deprovisioning is a risk mitigation technique to ensure that "authorization creep" does not occur, meaning additional and historical privileges are not retained. This avoids giving users access to data, assets and resources that are not necessary to fulfill the job role.

While people or users are normally thought of when authorization and access control are discussed, it is equally important to consider nonperson entities that are granted access to resources. A running process, computer program or device may be granted some level of access authorization and will often have a digital identity and store or handle factors of authentication (e.g., password or cryptographic key). When systems are designed to take maximum advantage of the cloud, they often leverage CSP-provided services as well as multiple small services or containerized applications to support elasticity. This introduces novel problems with the cloud, where systems might require dynamic provisioning and deprovisioning of access for large quantities of small services that may only exist for short periods of time. It also introduces challenges due to the potential number of nonperson entities that may have some level of access. A common failure with secure cloud design occurs when cloud customers do not realize or understand the level of access granted to a service or function or how to properly provision and deprovision access across the myriad of services they may be using. This has led to numerous compromises that allowed an attacker to manipulate the system or service after overly permissive access to a service or component of the cloud was either left on by default or not removed when unnecessary.

Centralized Directory Services

As when building a house or large structure, the foundation is key. The directory service forms the foundation for IAM and security both in an enterprise environment and within a cloud deployment. A directory service stores, processes and facilitates a structured repository of information, which is coupled with unique identifiers and locations.

The primary protocol in relation to interfacing with many centralized directory services is **lightweight directory access protocol (LDAP)**, built and focused on the X.500 standard. LDAP works as an application protocol for querying and modifying items in directory cloud service providers. LDAP is best thought of as a format for communication and messages related to directory services, but it still must be implemented correctly and securely (e.g., enabling TLS for secure communications), and improper implementation can introduce weaknesses.

Essentially, LDAP acts as a communication and message format protocol to interact with a common directory service—for example, Active Directory—in standard format. LDAP directory servers store data hierarchically, similarly to DNS trees/Unix file structures, with directory records' **distinguished name** (DN-the unique identifier for that record) read from the individual entries back through the tree, up to the top level.

Each entry in an LDAP directory server is identified through a DN. Access to directory services should be part of the identity and access management solution and should be as robust as the core authentication modes used.

Within cloud environments, directory services are heavily utilized and depended upon as the go-to trusted source by the identity and access management framework as a security repository of identity and access information. Again, trust and confidence in the accuracy and integrity of the directory services are essential. Cloud consumers may choose to integrate their cloud services with directory services they maintain onsite and fully control or utilize CSP-provided or third party-provided directory services or some combination. The exact design for an overall IAM architecture will drive the technical implementation, but the greater the number of directories (e.g., identity databases) the more complexity in management and the greater the difficulty of ensuring they are all secure. Conversely, complete reliance on a single centralized directory service requires that the service be highly available and highly secure.

Privileged User Management

As the name implies, **privileged user management** focuses on the process and ongoing requirements to manage the life cycle of user accounts with the highest privileges in a system. Privileged accounts typically carry the highest risk and impact, as compromised privileged user accounts can lead to significant permissions and access rights being obtained, thus allowing the user/attacker to access resources and assets that may negatively impact the organization.

A common error is over-provisioning access to administrative accounts. System administrators have historically been given many more access rights than necessary for their functions or are granted access rights that may be used legitimately on an infrequent basis. Both scenarios open the door to external

attackers targeting a privileged system or user accounts, as well as offering the potential for a catastrophic insider threat scenario. Privileged user management attempts to limit the exposure of highly privileged accounts, and in the most extreme case, privileges for access to a resource may be granted only when required and automatically revoked when no longer needed.

Privileged user management should, at a minimum, include the ability to track usage, authentication successes and failures and authorization times and dates, log successful and failed events, enforce password management and contain sufficient levels of auditing and reporting related to privileged user accounts.

Enhanced logging and monitoring may be enabled for privileged users, and additional access restrictions may also be applied. For example, if there is a privileged user account that is only intended to administer an application, that account should only have enhanced privileges for that application and should not have access to typical user services (e.g., email, web browsing). That approach would limit the exposure of the privileged account but may be impractical if the same administrator had multiple roles.

This is where **Privileged Account Management (PAM)** technologies provide value. These types of solutions can often be integrated with cloud services or may even be native to cloud services. They provide automated dynamic provisioning and deprovisioning of access on systems or services only when those permissions are required. They may also help enforce separation of duties for privileged access by enabling one user to control who has permissions to perform administrative tasks, while they themselves do not have that access, and the people performing privileged tasks may only do so once they have requested and been approved to perform a specific function.

With cloud services, some form of privileged user management is critical, whether automated with an integrated tool or managed solely as a process or monitoring activity. Exposure of administrative accounts that directly modify a cloud service can be catastrophic and remains one of the major concerns for cloud security.

Use of multifactor authentication and cryptographic authentication (digital certificate-based authentication) tied to hardware tokens is supported by most IaaS providers and is increasingly available for PaaS and SaaS providers, at least for

cloud consumer administrators. It is highly advisable to select a cloud service that includes built-in provisions for privileged user management or enhanced authentication security for privileged users and to enable that function in any existing cloud service subscription that supports it.

Data Deletion and Media Sanitization

Organizations must consider options for removing their data from any cloud service should the need arise. Cloud environments host multiple types, structures and components of data among various resources. For components within a multitenant environment, data deletion options are severely restricted, and many ultimately rely on proper implementation of mechanisms by the CSP. The cloud consumer has limited insight into how effectively data is deleted from the cloud-based service or resource. Reasons to delete data and sanitize relevant media include leaving a cloud service provider or migrating from one cloud provider to another. This can be especially difficult if it involves large amounts of sensitive data, and issues such as "vendor lock-in" and interoperability elements must be considered.

Aside from the hassle and general issues associated with reconstructing large data sets into a format that could be imported and integrated into a new cloud service or cloud service provider, the challenge related to secure deletion of data at the end of its life cycle remains a potential risk.

More information on data deletion policies is included in Domain 2.7.

Sanitization Options

To dispose of electronic records safely, the following examples may be employed:

- *Physical destruction.* Physically destroying the media by incineration, shredding or other means.
- *Degaussing.* Using strong magnets for scrambling data on magnetic media such as hard drives and tapes.
- *Overwriting.* Writing random data over the actual data. The more times the overwriting process occurs, the more thorough the destruction of the data is.

- *Cryptographic erasure.* Using an encryption method to rewrite the data in an encrypted format to make it unreadable without the encryption key.

Of the four examples listed, for cloud resources only cryptographic erasure is likely to be controlled by the cloud consumer. The CSP likely has processes and procedures for physical equipment and may employ a combination of the other techniques once equipment has reached its end of life or fails. This is typically transparent to the cloud consumer, but when evaluating a CSP, identifying that they have a destruction or media sanitization plan and have undergone third-party assessment of the destruction plan may be an important factor.

Physical Destruction

Digital information can be destroyed by disintegration, pulverization, melting, incineration or shredding. These are processes that entirely transform a storage device, such as a hard drive, into unusable media. The digital information, therefore, is 100% protected from exploitation.

Data Overwriting

While overwriting data multiple times is not inherently secure and does not make the data irretrievable, it can make the task of retrieval far more complex, challenging and time consuming. This technique may not be sufficient for highly sensitive, confidential or regulated information within cloud deployments.

When deleting files and data, they will become invisible to the user; however, the space that they inhabit in the storage media is made available for other information and data to be written to by the system and storage components as part of normal usage of the storage media. The risk with this is that forensic investigators and others with relevant toolsets can retrieve this information in a matter of minutes, hours or days.

Where possible, overwriting data multiple times will help to extend the time and efforts required to retrieve the relevant information and may make the storage components or partitions unattractive to potential attackers or those focused on retrieving the information.

In the absence of degaussing or physical destruction, which are not practical or realistic options for cloud environments, rendering data unreadable should be the approach taken. Lack of knowledge regarding the location of data eliminates data overwriting as a data destruction option. Adopting a security mindset, if the availability, integrity and confidentiality of the data can be restricted, the information becomes unreadable, which will act as the next best method for secure deletion.

Cryptographic Erasure

Since physical destruction, degaussing and overwriting are not applicable to cloud computing, the only reasonable method remaining for data sanitization is encrypting the data. The process of encrypting the data to dispose of it is referred to as digital shredding, crypto-shredding or cryptographic erasure.

Crypto-shredding is the process of deliberately destroying the encryption keys originally used to encrypt data. Since the data is encrypted with the keys, the result is that the data is rendered unreadable— unless the encryption protocol used can be broken or brute forced by an attacker.

To perform proper crypto-shredding, consider the following:

- The data should be encrypted completely without any cleartext remaining.
- The technique must make sure that the encryption keys are totally unrecoverable. This can be hard to accomplish if an external cloud service provider or other third party manages the keys.

A usually reliable way to sanitize a device is to erase and/or overwrite the data it contains. With recent developments in storage devices, most now contain built-in sanitize commands that enable users and custodians to sanitize media in a simple and convenient format. While these commands are mostly effective when implemented and initiated correctly, like all technological commands, it is essential to verify their effectiveness and accuracy.

Where possible (this may not apply to all cloud-based environments), erase each block, overwrite all with a known pattern, and erase them again.

When done correctly, a complete erasure of the storage media will eliminate risks related to key recovery, side-channel attacks on the controller to recover information about the destroyed key, and future attacks on the cryptosystem.

Key destruction on its own is not a comprehensive approach, as the key may be recovered using forensic techniques.

Network Security

Network security is a broad topic and is as important with the use of cloud services as in any other environment. The degree of integration for network security into a cloud service will vary from service to service based on the shared security model; however, some degree of network security is always inherently part of cloud computing. This section will introduce general topics in network security.

The CCSP should consider the shared security context and responsibility for execution with respect to any network security discussion. As with most things in the cloud, some aspects will be the responsibility of the CSP, some will be the responsibility of the consumer, and some will require both the CSP and the consumer to execute tasks.

When discussing networking security supporting a cloud service, network security needs or configurations from each of the following perspectives should be considered.

- *Network security for networks used to access the cloud (e.g., corporate network, public network).* Consider from which networks a device might access the cloud service. If access from purely public networks is permitted—for example, coffee shop Wi-Fi—it is imperative that appropriate controls are in place to ensure endpoints connecting to the service are trusted, have not been compromised and have implemented secure communications. Conversely, if a cloud service is configured to allow connections only from trusted networks (e.g., direct connection from corporate networks only) it can limit the exposure of a cloud service to some threats. In no way does the second example solve all network security issues; it simply limits exposure at the cost of limited access options. The first example, with its unrestricted

access, may expose elements of a cloud service to elevated risk but may be convenient or even required, depending on the use case for the service.

- *Security of transited networks (e.g., public internet, VPN).* Networks that may exist between a cloud consumer and a cloud service will introduce some risks. Even if sessions between a cloud client and cloud service are protected for confidentiality, the frequency and volume of traffic on the network may provide an attacker or malicious agent insight into activities or business processes through traffic analysis. Using technologies such as virtual private networks (VPN) can further encapsulate network traffic to make traffic analysis more difficult but will incur additional configuration and performance overhead.
- *Security at the CSP boundary.* What network security (if any) exists at the boundary between the CSP and its internet connection? This may or may not be transparent to the cloud consumer, but many CSPs do provide some level of monitoring, logging and threat prevention. The CCSP must consider how useful or relevant the protection provided by the CSP is to determine which additional controls the consumer should employ. In many cases, the cloud consumer will have the ability to configure or modify security settings at the boundary of their cloud. For example, with most IaaS, the cloud consumer has the option to set up and configure a virtual firewall between the consumer's virtual private cloud and external networks. There may be basic protections in place by default, but these would rarely be sufficient for most consumers without some level of additional configuration.
- *Security within the cloud infrastructure.* For IaaS, this is a critical element of cloud network security. This may involve configuration of network security groups, zero trust networking or other networking security approaches to harden the internal virtual network of the IaaS and prevent an attacker who has gained access to one portion from being able to move freely within the IaaS. The security concerns at this level for an IaaS are similar to configuring a secure corporate network infrastructure.

Network Security Groups

Depending on context, the term security group may mean different things. One potential meaning would be synonymous with access control group and be oriented towards users and what users can access. However, many cloud services

implement internal security controls, primarily on IaaS, but potentially in PaaS as well, that strictly control which things in the cloud can interact with others over the virtual network. These are often referred to as network security groups and can function, depending on the service, similarly to a partitioned traditional network that has multiple network segments and strict rules over what communications are permitted to flow between segments.

In this context, network security groups may be configured to explicitly allow or deny connections or communications between entities such as virtual machines and cloud services in the cloud or to define the level of communication and exposure allowed between cloud-based entities and external networks.

Improper configuration of network security groups that control or limit communications can have a detrimental impact on the security of the cloud.

Traffic Inspection

Traffic inspection occurs when a sensor of some type (e.g., firewall, IPS, gateway, agent software) analyzes network traffic to determine if it is allowed, properly formatted, free from known malware, and not exhibiting patterns consistent with attack methodologies.

Basic traffic analysis can occur when the sensor only has access to the Internet Protocol addressing but provides limited insight into what any particular packet on the network contains. Traffic inspection takes the basic analysis one step further and opens the data payload and reads the contents.

When considering architectures for the cloud, it is important to consider where sensors or components that can see network traffic and generate log data are placed, and how information can be retrieved from them.

If end-to-end encryption is used, the data payload may be encrypted and not available for the traffic inspector sensor to analyze. Since common attack methodologies encrypt their data payloads to avoid inspection (and thus detection), this can be challenging. For traffic inspection to occur, the sensor must have the ability to read the data. This can be accomplished by placing the sensor in a location where unencrypted traffic is available for inspection, or by using techniques to decrypt the traffic, read the payload and then re-encrypt the payload.

The second is made problematic by forward security mechanisms built into many modern communication protocols (e.g., TLS 1.3) that are explicitly designed to prevent an attacker from doing what we want our traffic inspection security sensor to do.

There are mechanisms that can be employed for enterprise systems that can allow an authorized security sensor (e.g., IPS) to gain access to encrypted network traffic for inspection. However, they can be difficult to configure and may not be compatible with some cloud services.

Geofencing

Geofencing, or **geoblocking**, refers to any technology that can relate digital users to their actual physical location, or a close approximation thereof, and may be configured to act if the location does not correspond with a specific geographic boundary in the physical world.

Geofencing can be used to allow or deny access to cloud resources, determine potential threat levels of someone connecting to a service, or facilitate trusted access. However, the effectiveness of any geofencing technology is limited by the level of assurance that a service has over the physical location of someone connecting over the internet. Geofencing may also be limited by the mechanisms available to determine actual physical location with appropriate levels of certainty.

In the most basic form, the IP address from a network connection can provide a rough approximation of the physical location of the entity connecting. IP addresses are mapped to specific Internet Service Providers (ISP), who typically have assigned addresses by geographic location. This can provide a rough idea of the country or region someone is in. This is considered a low-quality geolocation method, however, and is relatively easy for an attacker to spoof using a public VPN service or by using compromised systems in other localities. However, it can be useful for bulk filtering traffic, and is used in many geoblocking schemes, where traffic from an entire region can be blocked, or institute-enhanced logging as one of many deployable controls.

As an example of a high-quality geofence, assume a company issues mobile devices to employees. The devices contain a hardware root of trust such as TPM and have

secure boot enabled; they also have a mobile device management (MDM) software agent installed. If the device has a global positioning system radio receiver, the position of someone connecting from that device can be determined with a high degree of certainty. Since the hardware is controlled and has tamper protections (TPM and secure boot), there is good assurance the OS is trusted, and if the MDM can determine the OS is configured properly, up to date with patches, and has not been tampered with while running, the MDM can provide fair assurance that an application accessing the device radio and obtaining a global positioning satellite signal is not being spoofed or tampered with. Since the device is registered with the MDM, there is cryptographic assurance that the device originating a message is the known, registered device and that it can be trusted to provide accurate geolocation information, at least with some degree of confidence. While this example may seem complicated and requires numerous parts to work properly, it is realistic and can be employed with technologies natively included in some cloud services today by enabling and configuring them. However, if not integrated into the cloud service, attempting a maximal solution could be costly and require a significant amount of effort to deploy.

Many organizations or applications will employ some degree of geofencing for mobile connections. In the example above, it was assumed that there was a higher degree of confidence in accurate location information because of the mechanisms that provide some degree of trust in the device itself. If these are not present, or present in a limited form (e.g., BYOD without MDM installed), trust in the accuracy of the location should be reduced accordingly. There are a range of solutions available that employ geofencing or geolocation, many integrated with cloud services, but the CCSP should always consider and evaluate the degree of confidence that should be placed in any geofencing used for security. In some cases, high confidence may be warranted, but in others, it may provide little effective value.

Zero Trust Network

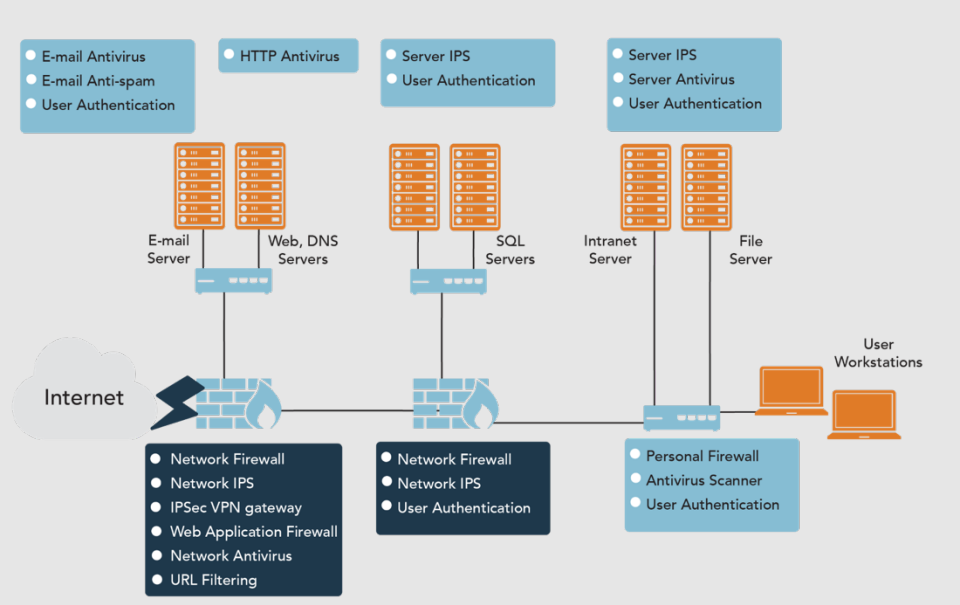


Figure 1.24: Zero Trust Network

Trust nothing, verify everything, and disallow anything not explicitly allowed. These are the basics of zero trust networking.

Zero trust networking is not new, but practical employment of zero trust on traditional computing systems has increased in recent years. Industrial control standards from 40 years ago introduced the concepts of zones and conduits, which read much like many vendor documents on zero trust solutions today. However, those standards were based on industrial control systems that might be installed with minimal changes for a decade or more, and the exact communication requirements were well known, which is not comparable to a general-purpose computing environment. Zero trust has been slow to emerge as a practical security approach on traditional networks and computing systems largely because of the difficulty configuring a true zero trust environment. With legacy industrial controls, elements that needed to interact were placed on the same physical connection, and information from that network was not allowed to flow to others unless it exactly met a specification for doing so. This tends to be impractical on a general-purpose computer system or network, where a user or application needs to do different

tasks at various times. Predefining the complete set of allowable communications or data exchanges has been impractical, as adapting to change was slow and might require significant reconfigurations.

However, faster speeds in computer hardware, better software systems and improved automation have made zero trust architectures practical to install and maintain, at least to a much greater extent than previously. Since cloud services rely heavily on virtualization, implementation of zero trust in cloud architectures may be easier in many cases than attempting to retrofit an existing on-premises architecture.

The graphic shows some general components on a traditional network. However, they might also be virtual machines within an IaaS. Each component within the infrastructure has appropriate security controls or tools, and boundaries are placed between elements of the architecture. The firewalls depicted in the diagram enforce separation between components that do not need to directly interface on the same network segment and would filter traffic attempting to transition from one segment to another. Every device has its own software firewall installed and would disallow any traffic to other systems unless that communication has been authorized.

Some cloud-based systems and infrastructure can take this a step further and virtually isolate every component on its own effective network segment; nothing is permitted to cross outside of its authorized segment unless it has been explicitly allowed to do so. While there is a challenge in initially configuring something like this, the more problematic issue is maintaining it and allowing it to work, especially when any type of change occurs. In the past, this was where zero trust was difficult to employ: It was difficult to scale the trust boundary down to the level of individual applications. Now, with modern cloud architectures, where many of the internal components may be containerized microservices, and strictly from a communication perspective, it begins to look a little bit like the industrial control systems of 40 years ago. It may only need to communicate with one or two other services, and the allowed communications may be well known with limited changes likely. Since something like a containerized microservice is only intended to perform a narrowly defined task, its communication can be narrowly defined, as it is consistent with a zero-trust design.

Zero trust may remain impractical at the most granular level for many systems or applications, but it is advisable to apply the zero-trust model to the greatest degree possible, then to extend that model over time as it becomes more practical.

Computing Components in the Cloud

This section will introduce some common, security-relevant components that might be found in many cloud architectures. Some, like virtualization security, will be an inherent risk in any cloud architecture, while others, such as serverless technology, may or may not be present in a specific cloud infrastructure.

The elements in this section will introduce the concepts, many of which will be addressed in more detail or with a different perspective in later sections.

Virtualization Security

Virtualization security is relevant to any cloud infrastructure. However, it is largely a CSP responsibility as part of the security of the cloud, regarding which the CSP might share little insight with the cloud consumer. Since virtualization is a core technology for any cloud, the underlying virtualization layers of the architecture must be properly configured and resilient against attack. A third-party certification or assessment of a CSP may provide some, but likely minimal, insight into how well the CSP operates the underlying virtualization infrastructure of the cloud.

While this should be considered a risk for any cloud service, in some instances of IaaS the cloud consumer may have direct control over virtualized components, including configurations that affect how secure the component is or how it interacts with the underlying architecture. In that respect, there may be a small amount of virtualization security that is a shared responsibility or purely a customer responsibility under IaaS. However, SaaS and PaaS offerings may provide little or no interaction with the virtualization layer, and the customer may have no knowledge of how it is configured.

Hypervisor Security

The hypervisor is the component of the virtualization infrastructure that interfaces with the underlying infrastructure and presents virtualized components (e.g., virtual hard drive, virtual processor) to guest OSs residing in the virtualized environment. Hypervisor security is almost always the sole responsibility of the CSP and is one of the most important tools to enforce separation between tenants on a public cloud. As such, it is susceptible to attack, and if compromised, could allow the attacker to access everything the CSP would normally be able to, and possibly to other tenants' data or systems as well.

Hypervisors tend to be small pieces of software written for a single task—the management of virtual resources. While they tend to be secure and robust and are typically tested heavily, they are also one of the largest potential risk areas of any cloud infrastructure, should it be successfully attacked.

It is normally up to the CSP to manage, maintain and monitor the security of hypervisors in the cloud environment.

Container Security

Hypervisors allow virtual machines to run in a virtual environment by presenting virtual resources to them as if the virtual resources were physical resources. Virtual machines running on a hypervisor tend to behave and operate consistently with that same machine running directly on physical hardware. A virtual machine typically has an operating system and all the components found on the physical version of the VM.

Containers, however, are essentially virtualized applications. A **containerization** platform bundles all the resources and dependencies needed for an application to run into a container. In that context, the containerized application can run independently of anything else, as it has everything it needs to run in the container, but nothing else. The container will not contain a full operating system and can only execute on a platform configured for that container type. However, since it does not have an operating system, and is a small-form factor compared to a full virtual machine, containers can be stopped, started, created or destroyed nearly instantaneously. If there is a master image of a containerized application to be run,

the containerization platform will simply create an instance (copy) of the container, run it, and when completed, delete the copy. That is an example of ephemeral computing realized through containers.

Much like the hypervisor, the containerization platform orchestrates and executes the containers. Security of that platform is paramount in a containerized environment. Containers also share the same OS or platform instance with other containers, so just as the compromise of a hypervisor can be catastrophic, the same issue may apply to the containerization platform.

The containerization platform will isolate the container's contents from anything outside and affords a good level of security. However, misconfiguration or direct compromise of the containerization platform can result in significant loss.

Where the containerization platform and container security fall in the shared security model will depend on the cloud service offering with which it is integrated. While some CSPs offer container platforms that could be classified as PaaS, other providers give significant control to customers for their own instance of a containerization platform, which requires the cloud customer to ensure it is configured properly for their needs.

The CCSP should always determine to what degree the container platform and container security are a CSP or cloud consumer responsibility and apply appropriate configurations and controls. Different cloud providers may offer significantly different solutions and levels of control for containerization.

Ephemeral Security

The example from the container security section also covers one element of ephemeral security. **Ephemeral computing**, or nonpersistent computing, is an approach with virtual systems or containerized applications where the system is designed not to require information or state to be maintained between operations. Ephemeral computing is explicitly designed to be created and deleted without having to retain information from the deleted copies. This does not mean information is not retained—there will be monitoring and logging outside of the ephemeral component, and the ephemeral component may exchange or offload information as part of a transaction—but once it has completed its task, it can be

deleted, and a new copy created from a master image when the task is required in the future.

Ephemeral systems have some security advantages in that they tend to be short-lived, and since no state will be retained, even if the systems are compromised while running, attackers have a short time window to achieve their goals. This does not mean that ephemeral systems are inherently secure, and protections for data while resident on the systems must be considered, as must be protecting the functioning of the ephemeral components' form manipulation while in operation. However, ephemeral systems do tend to provide protection against many types of persistent threats and make successful attacks difficult.

Ephemeral systems or applications are often created when needed from a master copy. A single copy or hundreds can usually be created rapidly, with little overhead. Once each copy completes its task, it is deleted. Since whatever happened in that copy is now gone, it is often necessary to provide external logging and monitoring, and there can be challenges with retaining necessary information about the operation of individual copies if the system is not designed to do so.

As an example, consider a case where shipping costs for the contents of an e-commerce shopping cart must be calculated. This problem only requires a small set of information to calculate (e.g., shipping location and product information such as dimensions and weight). Perhaps there must be a level of elasticity as well, as there could be any number of internet-based customers using the website at the same time. If this organization builds a lightweight, containerized microservice that does nothing but perform one calculation based on a standard input format then provide the results in a standard output format, the application does not need to retain state from one transaction to the next. If 1,000 copies are needed, it can easily be done, and because the calculation only requires an input and the output is provided to another component for retention, each copy can be deleted as it finishes its calculation. A new one can be created dynamically when needed. This approach can support elasticity in a cloud-based application that can easily grow or shrink as demand changes.

Serverless Technology

Serverless technology is not serverless. Specifically, the servers are abstracted from the user of the serverless technology. Organizations do not need to install, configure, maintain or otherwise deal with physical or even virtual servers, server operating systems or any of the other overhead tasks associated with running a complex IT system.

An application written for a serverless platform typically issues commands or requests to the platform using a predefined protocol or API. The platform then executes that command and returns the results. Since the backend systems are transparent to the user of the service, the service can be expanded or modified as necessary by the operator without impacting the service users. A common type of serverless technology is **Function as a Service (FaaS),** which is available from many cloud providers. The organization then tells the service what it wants, and the service figures out how to resource it.

Serverless technology will typically employ stateless ephemeral, microservice-based architectures using a containerization platform. This allows for the rapid scaling that is inherent in many cloud services. While not a new capability, this is an area that still sees regular advancement in capability and more diverse use cases being applied in the cloud.

As with any cloud service, it is incumbent upon the CCSP to understand how a serverless service offering falls in the shared security model. In most cases, responsibility for overall security will fall on the CSP, but the cloud consumer may write commands or code that will be executed on the serverless architecture. Ensuring the commands or code are securely designed and requests to the service are properly secured is the responsibility of the cloud consumer.

Role-Based Access Control

Role-based access control (RBAC) is an AC policy that restricts information system access to authorized users. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) needed to perform operations on organizational information systems associated with the organization-defined roles.

Access will be granted by the owner and applied with either cloud-based identity and access management (IAM) tools or the organization's own IAM tools.

RBAC can be applied by degrees to meet the needs of an organization, as the figures below illustrate. The top portion of the figure below shows an organization that is not using any form of RBAC. Individual users are granted permission to run (load and execute) certain sets of applications or programs. The organization may not want its accounts payables staff developing software, so on a per-user ID basis, they block them from being able to run integrated development tools such as Visual Studio. The lower portion of the figure below shows a limited use of roles, associating applications to specific roles. Thus, the accounts payable team member role has permission to run QuickBooks (Application 1, Role A), but the developers (Role B) can run other apps for software development and test them. In this example, each individual user ID is associated with one or more specific roles. This allows applications to be used irrespective of any roles assigned to users; for example, all users may be able to run Firefox or Chrome.

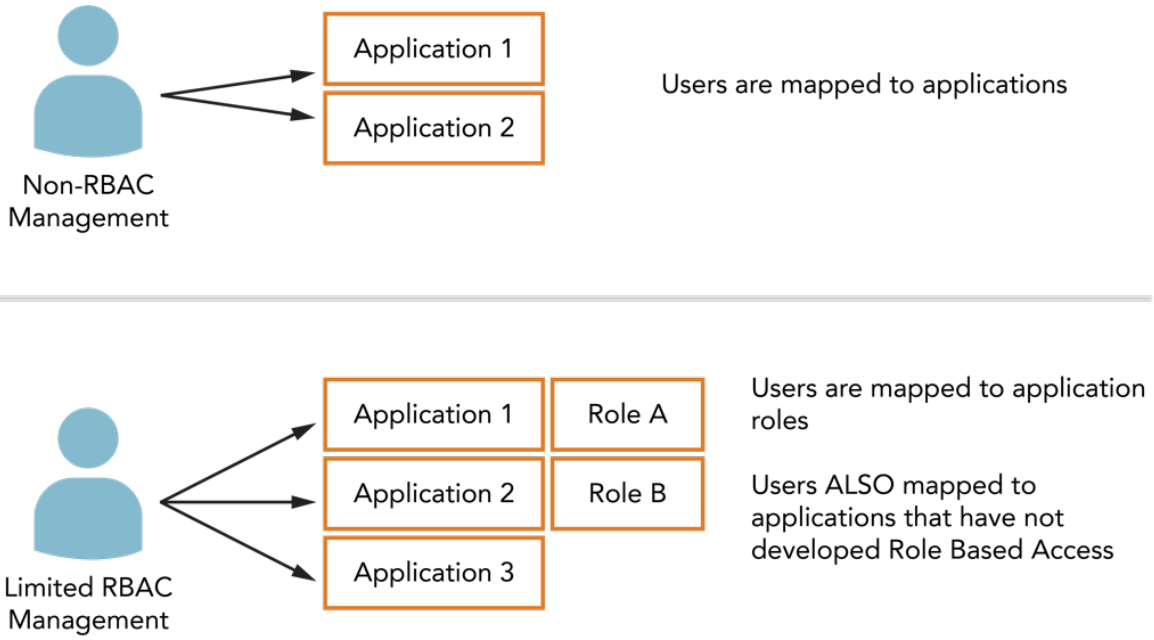


Figure 1.25: RBAC Use Cases: None and Limited

The next figure shows more extensive use of RBAC. The hybrid RBAC management case (top portion of the figure) illustrates a hybrid use case, which shows how individuals may have one or more roles, each of which is permitted to use one or more specific applications. The rights and privileges associated with Role A in this example would probably be different from those involved in Role B, even if the same application is being used in both roles. A point-of-sale application, for example, may have roles defined for a salesclerk or a sales supervisor, but only the supervisor role would be able to use the price override or transaction void features. The lower portion of the figure below shows a full implementation of RBAC, with all user IDs first mapped to roles, then those roles mapped to applications.

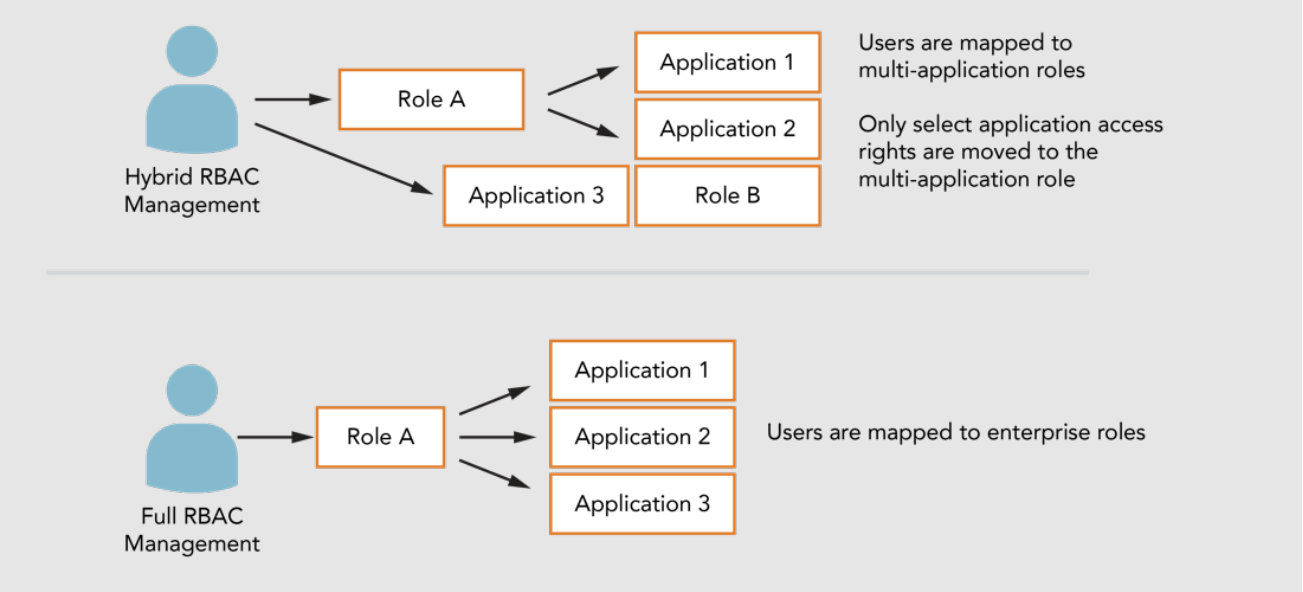


Figure 1.26: RBAC Use Cases: Hybrid and Full

The next figure shows a few of the many ways RBAC can be used.

- *None.* Access to specific apps and their data is not protected by anything role-based. Individual privileges must be defined and managed.
- *Limited.* Some apps and their data are RBAC-protected and restricted to specific, defined roles. Others are not. In this case, office productivity apps and browsers are not attached to RBAC.

- *Full.* Every app, including office apps and browsers, requires role-based permission to be accessed. An HR manager signs on in their HR role to access personnel files. To do office correspondence, they sign out of that role and sign in again with their office role.
- *Hybrid.* Hybrid can be any combination of features.

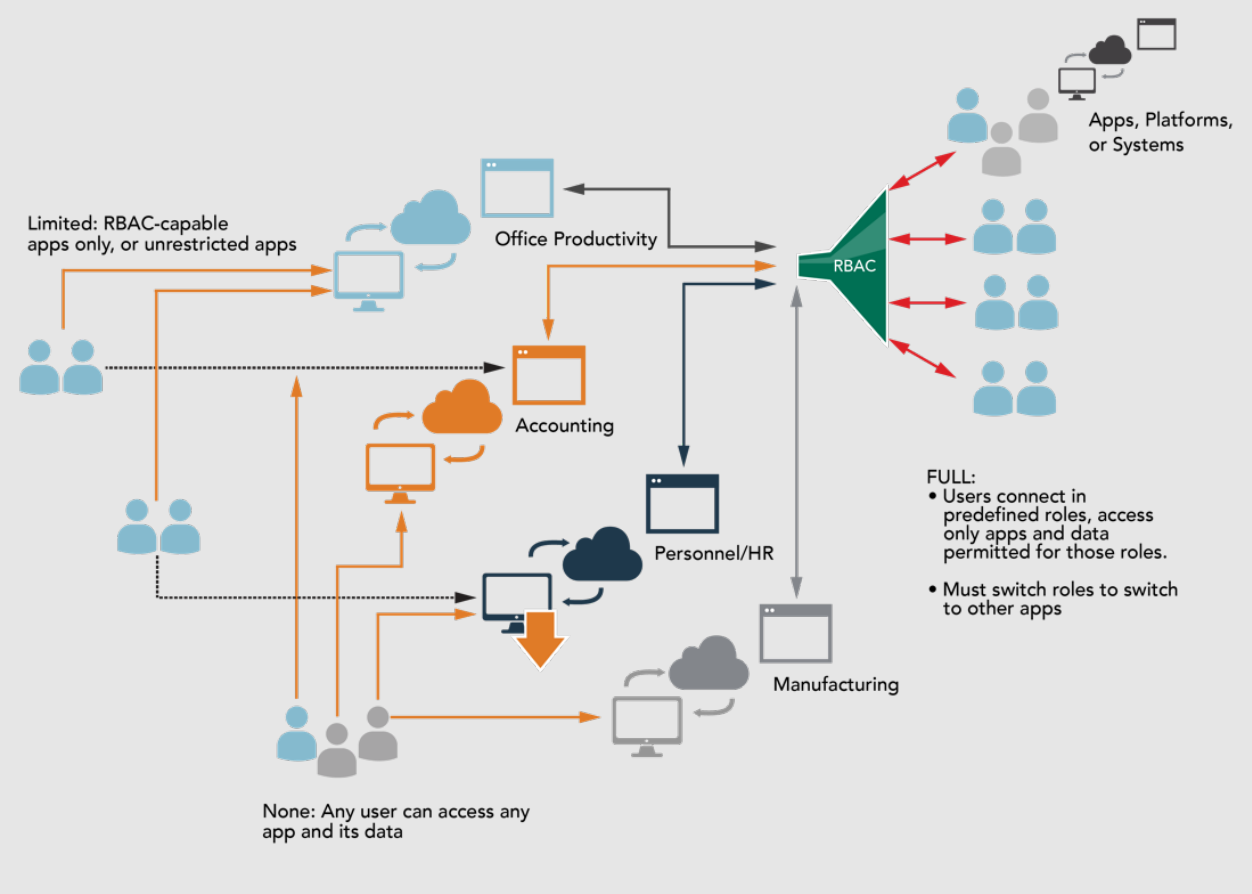


Figure 1.27: RBAC Implementation Options

Cloud environments often include an administrative capability to change roles. For example, in AWS, this is called “assume role” and is valid for all identities.

Common Threats

Threats to **cloud applications** and resources are as many and varied as the types of cloud services and capabilities that exist. Cloud-based capability inherits the risk

of its component pieces, and in that way, is no different from any other computer resource. However, some of the capabilities of the cloud, which make it an attractive approach to solving problems, may also introduce new risks or significantly enhance existing risks if not treated properly. Conversely, some inherent features of the cloud tend to make cloud-based capabilities more resilient against common threats that may impact noncloud capabilities, particularly those threats that might impact availability.

A noncomprehensive list of cloud threats, from the cloud consumer point of view, is listed below, however, we will also be addressing cloud threats throughout the course. Many of the threats listed exist in noncloud environments but may be of special concern for the cloud:

- *Data breaches.* Data breaches occur whenever sensitive information is improperly disclosed, or in some cases, there is evidence it could have been disclosed. The always-on, always-connected nature of the cloud increases the potential risk for data breaches that are more widespread or widely distributed than might be the case in noncloud systems. Many of the threats listed in this section may contribute to data breaches as well.
- *Improper configuration.* A major threat to cloud-based capabilities is weak or poorly implemented security due to improper configuration of a resource. The resource could be a cloud service that is not configured properly for the purpose it is being used for, or a customer application that has not been properly configured for use in the cloud. Improper configurations are particularly risky in the cloud since they may be more exposed or accessible to potential threat actors and issues arising from improper configuration may be more significant.
- *Interface attacks.* This can include any type of injection or manipulation attack against any type of exposed interface. Threats may be unique to the types of interfaces utilized, but they are often related to improper exposure of interfaces to external access, or either lack of proper identification and authentication on interfaces or improperly configured identification and authentication.
- *Identity and Access Management failures.* This can include loss of credentials through theft or improper exposure as well as improper configuration. Attackers will often attempt to guess or obtain credentials that will allow access to resources. If applications are not properly configured and if strong

authentication mechanisms are not used, the connectivity of the cloud can make IAM failures more damaging. This issue is a potential problem for both human operated and nonperson entity IAM, and not only includes interfaces used directly by humans (e.g., web page) but machine to machine or Application Programming Interface (API) connections.

- *Application flaws.* Application or software flaws exist in all software, regardless of whether it is used in the cloud or on-premises. However, application flaws may be more exposed to external attack in the cloud, especially if an application or application interface is improperly exposed due to a design error or improper configuration of the cloud platform.
- *Improper use, configuration or implementation of cryptography.* Cryptography can be used to protect data confidentiality and integrity in many scenarios. However, not every use of cryptography will protect data from all potential threats. The cloud can complicate the use of cryptography as it may be necessary to use it in diverse ways to protect data from different threat sources, which can include the CSP and platform. This can lead to cryptographic solutions that do not protect the right things from the right threat sources or improperly expose keys or secrets to threat sources, including, and especially, the CSP.

Security Operations and Hygiene

Security operations and general hygiene will be covered in more detail in Domain 5. Security operations are the activities conducted by an organization to maintain system security over time. Security operations typically include the monitoring of maintenance activities that are relevant to maintaining security. These activities with security relevance may be referred to as security hygiene and include things such as monitoring system configurations and patching systems. A well-designed and well-implemented system or architecture naturally degrades over time if hygiene activities are not conducted consistently and well. Security operations include the activities to manage or monitor hygiene activities but also include incident response, disaster recovery, configuration management, threat hunting and many other tasks. While not all hygiene activities are conducted by security staff or a security operations center (e.g., patching may be conducted by IT operations), they should typically be monitored or tracked by security operations to

ensure security effectiveness is maintained (e.g., security operations track patch deployment status).

A noncomprehensive list of typical security operations or hygiene activities is listed below:

- Critical asset identification and tracking, including data assets
- Monitoring and log management
- Incident response
- Recovery and remediation
- Security related root cause analysis
- Compliance

Understand the Design Principles of Secure Cloud Computing (1.4)

Objectives

- Describe key security considerations for each service model.
- Evaluate cloud computing ROI and KPI metrics.

Overview

In cloud computing, security is a shared responsibility between the CSP and the customer. The following section focuses on design principles of secure cloud computing, such as business continuity and disaster recovery, restoration, functional security requirements, and security considerations for IaaS, PLaaS and SaaS.

Cloud Secure Data Life Cycle

Secure data in the cloud has a life cycle. To manage data effectively and keep it secure, it's important to understand the common phases of data life cycle models.

The six phases of the data life cycle are: creation, storage, usage, sharing, archiving, and destruction. While the life cycle is described as a linear process, data may skip certain phases, or even switch back and forth between them.

Domain 2.1 includes more information on the secure life cycle phases.

Cloud-based Business Continuity and Disaster Recovery Planning

All major cloud service providers offer **Disaster Recovery as a Service** (DRaaS) that organizations can utilize in case of a disaster in an on-premises situation. There are several characteristics of the cloud environment to be considered for a **Business Continuity and Disaster Recovery** (BCDR) plan. They represent opportunities as well as challenges. To do that, it pays to have a more detailed look at three scenarios:

- On-premises, cloud as BCDR
- Cloud consumer, primary provider BCDR
- Cloud consumer, alternative provider BCDR

For more information on BCDR, refer to Domain 3.5.

On-Premises, Cloud as BCDR

The first scenario is an existing, on-premises infrastructure, which may or may not have a BCDR plan already, where a cloud provider is considered the provider of alternative facilities should a disaster strike at the on-premises infrastructure. Workloads on physical machines may need to be converted to workloads in a virtual environment. It will also be important to review the speed with which the required resources can be made available.

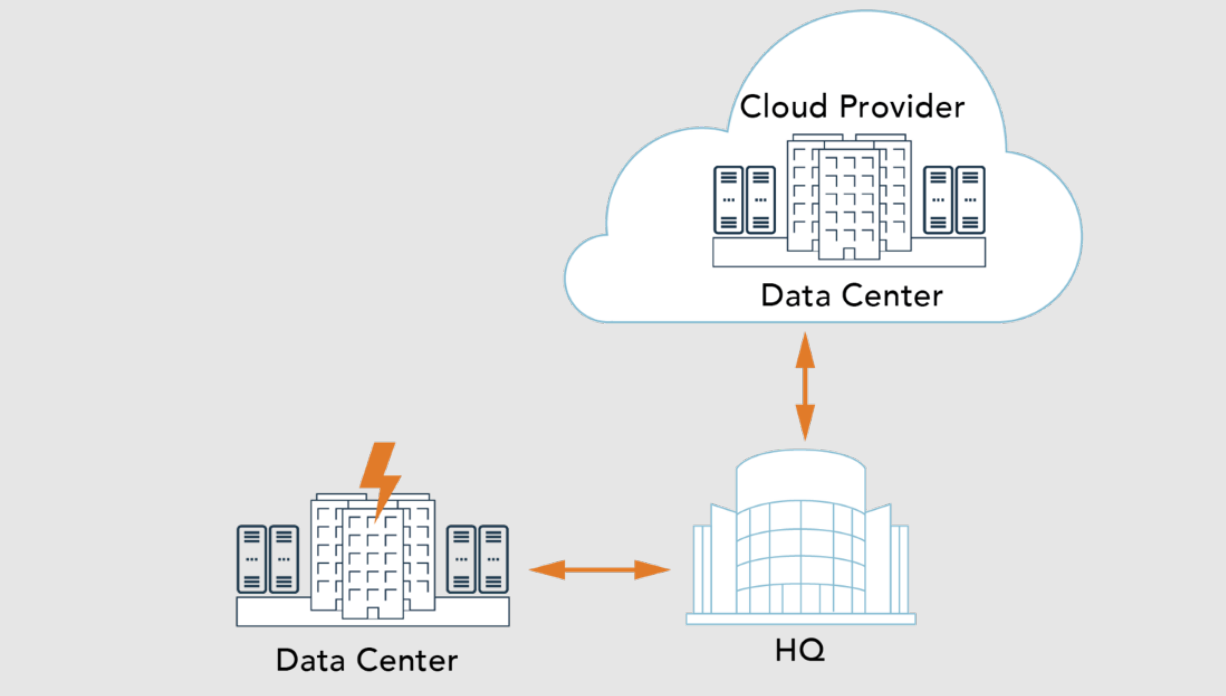


Figure 1.28: On-Premises, Cloud as BCDR

Cloud Consumer, Primary Provider BCDR

In the second scenario, the organization has migrated from on-premises infrastructure to a cloud provider. The risk being considered is that of a failure of part of the infrastructure of the cloud provider—for example, one of their regions or availability zones. The business continuity strategy then focuses on restoration of service or failover to another part of that same cloud provider infrastructure. Even though this scenario relies heavily on the resources and capabilities of the existing cloud provider, a reevaluation of the provider's capabilities is necessary because the BCDR strategy is likely to require novel resources and functionality. As examples, consider load-balancing functionality and available bandwidth between the redundant facilities of the cloud provider.

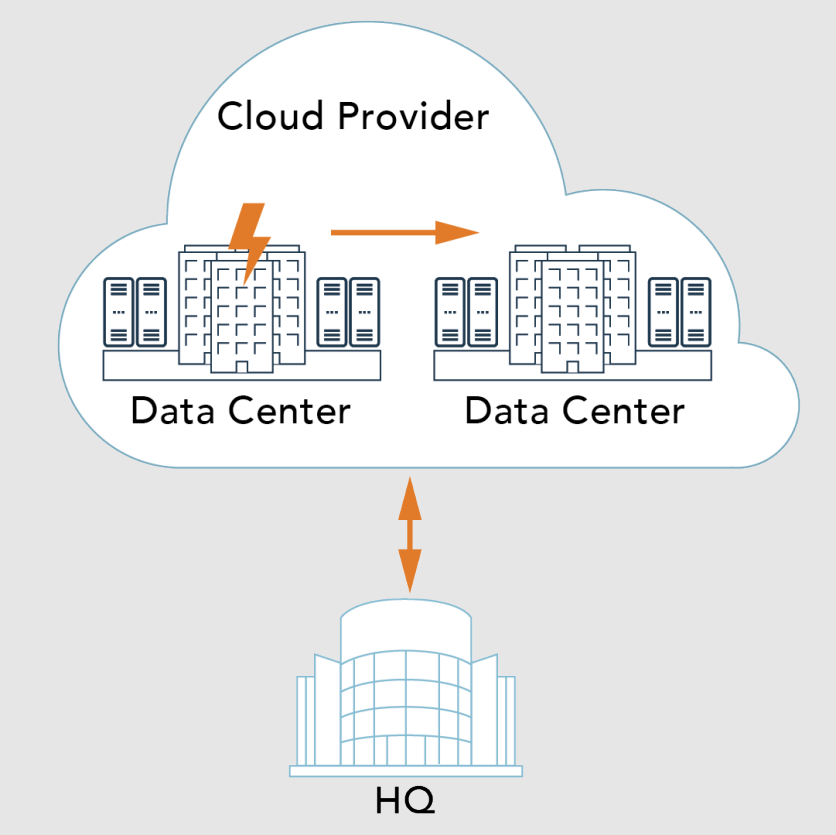


Figure 1.29: Cloud Consumer, Primary Provider BCDR

Cloud Consumer, Alternative Provider BCDR

The third scenario is like the second scenario, but instead of restoration of service from the same provider, the service must be restored from a different provider. This also addresses the risk of complete cloud provider failure. Disaster recovery, almost by definition, requires replication. The key difference between these scenarios is where the replication happens. This is like the selection of a new provider. It might be helpful to reconsider the selection process that was done for the primary provider. Data portability and interoperability are at elevated risk when using two different cloud providers. Frequent nonproduction tests are recommended to ensure a small impact on business applications.

The speed with which the move to the new provider is made should be a primary additional concern. In the case of protecting against the failure of a SaaS provider, it is likely there will be an impact on business users because the functionality they are used to is unlikely to be equivalent to the functionality of the failing SaaS provider. It may prove worthwhile to involve the business users as soon as possible so that they will be able to assess the direct residual risks to the business.

In all cases, a proper assessment and enumeration of the risks that BCDR protects against, risks inherent in BCDR and potential remaining risks are important for designing adequate BCDR strategies and making balanced business decisions.

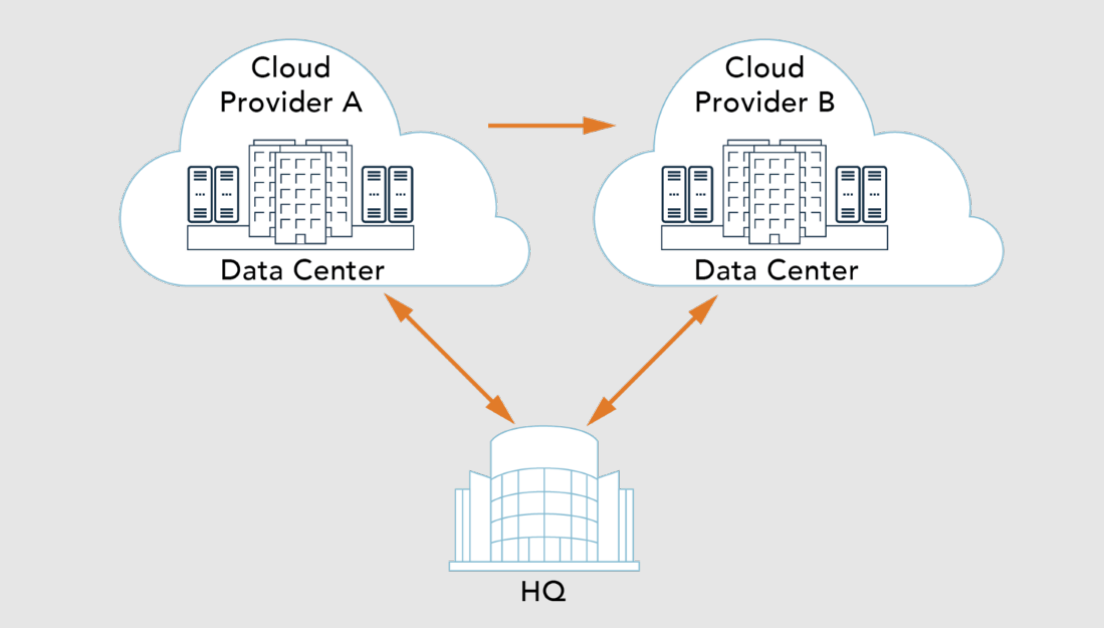


Figure 1.30: Cloud Consumer, Alternative Provider BCDR

Recovery and Restoration

Recovery and restoration are separate activities that share a common timeline. Recovery activities are designed to recover the systems to an operational state as soon as possible after a declaration of disaster has been made. Restoration activities are designed to migrate the business back from recovery mode.

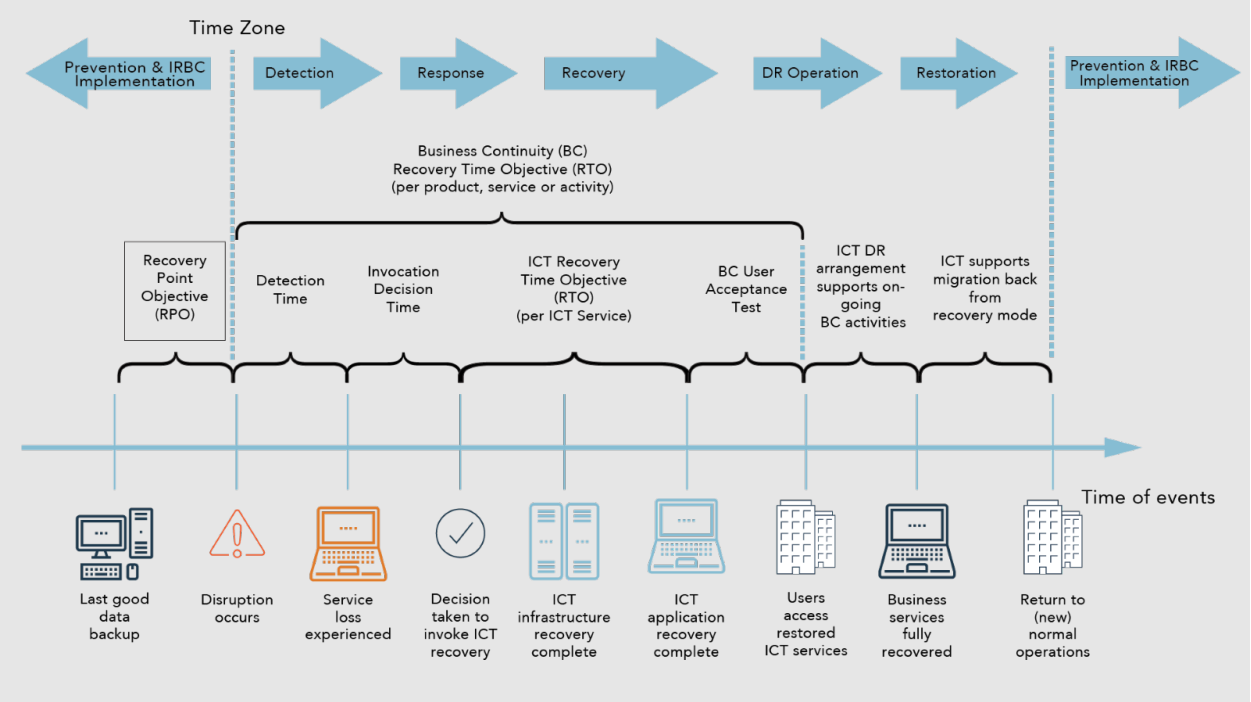


Figure 1.31: Recovery and Restoration Timeline Milestones During a Disruption

Recovery

As each BCDR strategy addresses the loss of important assets, replication of those assets across multiple locations is assumed. The relevant locations to be considered depend on the geographic scale of the calamity anticipated. Power or network failure may be mitigated in a different zone in the same data center. Flooding, fire and earthquakes probably require locations that are more remote. Switching to a different cloud provider will also likely impact the sites of operations.

Not all service models allow the same breadth of components. In other words, it would be unlikely that a SaaS consumer would carry out data replication at the block-storage level.

Data Replication

This diagram depicts the main components of a typical failover architecture.

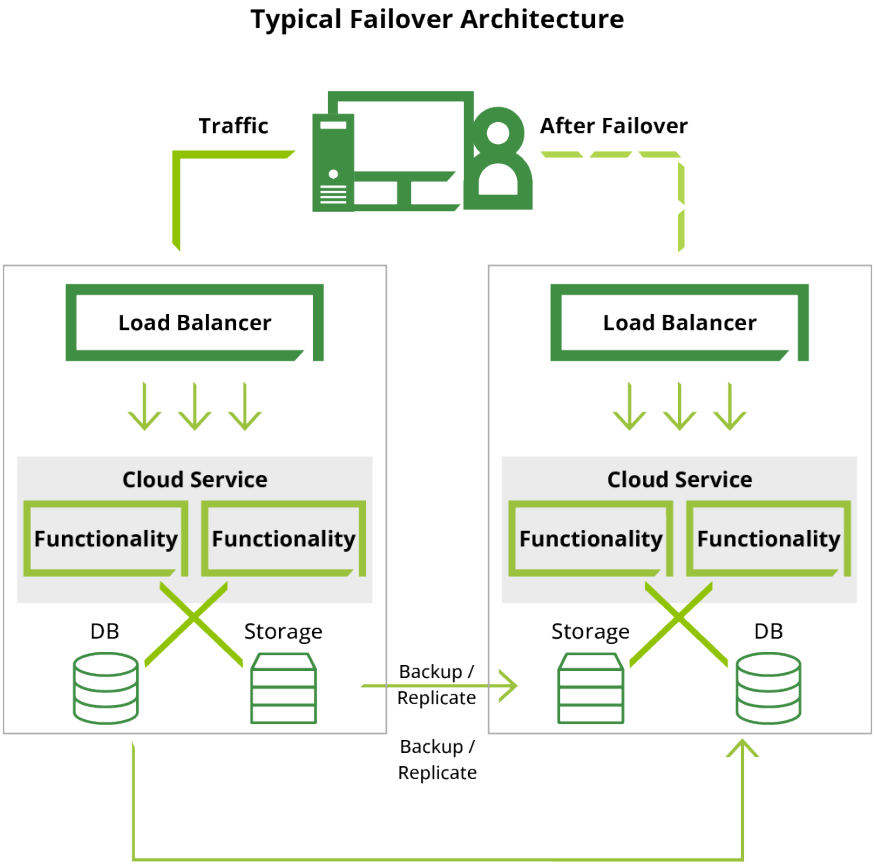


Figure 1.32: Typical Failover Architecture

Data replication concerns maintaining an up-to-date copy of the required data at a different location. It can be done at several technical levels and with different granularity. For example, data can be replicated at the block level, the file level and the database level. Replication can be in bulk or on the byte level and done by file

synchronization, database mirroring, daily copies, etc. These alternatives can differ in their recovery point objectives, recovery options, bandwidth requirements and failover strategies.

Each of these levels allows the mitigation of certain risks, but not all risks. For example, block-level data replication protects against physical data loss but not against database corruption, and it will also not necessarily permit recovery to a different software solution that requires different data formats.

Furthermore, backup and archive are traditionally also used for "time machine" functionality, which can mitigate risks related to accidental file deletion and database corruption.

Beyond replication, there may exist an opportunity to rearchitect the application so that relevant datasets are moved to a different provider. This modularizes the application. Examples of components to split off include database as a service or remote storage of log files. This will make this data resilient against provider failure, although a new dependency is introduced.

In contrast with IaaS services, PaaS and SaaS service models often have data replication implicit in their service. However, that does not protect against failure of the service provider, and exporting the important data to external locations may still be necessary. In all cases, selecting the proper data replication strategy requires consideration of storage and bandwidth requirements.

Restoration

Disaster recovery ends in a return to normal. In case of a temporary failover, the return to normal means going back to the original provider or in-house infrastructure.

Alternatively, a return to the original provider may no longer be possible, and in that case the DR provider becomes the "new normal." In all cases, it is wise to document lessons learned and clean up any resources that are no longer needed, including sensitive data.

The whole BCDR process and, in particular, the failover event, represents a risk mitigation strategy. Practicing it entirely or in part will strengthen the confidence in

this strategy. At the same time, such a trial run can result in a risk to production. These opposing outcomes should be carefully balanced when developing the BCDR strategy.

At this point, the strategy should be concrete enough to turn into an implementable plan. An organization should next focus on ICT readiness for business continuity (IRBC), which will foster a systemic process to prevent, predict and manage ICT disruption and incidents that have the potential to disrupt ICT services. This can be best achieved by applying the Plan, Do, Check, Act (PDCA) cyclical steps as part of a management system within IRBC. In this way, IRBC supports BCM by ensuring that the ICT services are appropriately resilient and can be recovered to predetermined levels within the time scales required and agreed upon by the organization.

Business Impact Analysis (BIA)

The Business Impact Analysis (BIA) is a key component of any cloud transition or the use of any cloud service. A BIA attempts to predict or calculate the consequences of any disruption to a business function. Disruptions could be caused by people, process or technology (or any combination). While not strictly technical in nature, a BIA will map business functions to potential impacts from disruptions. When combined with additional mapping between business functions and supporting architecture (people, process, technology, services), the BIA provides insight to how disruptions affecting any component of the architecture could impact the business functions of the organization. This is particularly important to mapping how potential cloud service disruptions could impact critical business functions.

The BIA is not an information security task in many organizations, but it is critical to information security as it often sets protection needs for confidentiality, integrity and availability.

Cost Benefit Analysis

When selecting cloud services, a Cost Benefit Analysis (CBA) should always be performed to ensure selection or transition to a service offering is in an organization's best interest. A CBA can be performed in a variety of ways using various methodologies, but the sum result is to measure the benefits of one

approach over another. This could include the benefits of one cloud service over another or from using a traditional IT infrastructure compared to a cloud-based infrastructure.

CBA methodologies must be systematic, repeatable and consistent. The primary goal is to compare strengths and weaknesses of two or more approaches to solving a problem or providing a capability. CBA methodologies for cloud should include as many factors as feasible and, where useful information is available, quantify actual benefits to the greatest extent possible.

For example, in moving from a traditional environment to the cloud, one factor in the CBA would be potential workforce costs. The analysis could determine that moving infrastructure to the cloud could reduce the need for data center operators but that moving to IaaS may not reduce the need for system administrators and could include a need for retraining or enhanced administrative training for existing staff. The analysis would attempt to determine the net benefit (which could be negative) for the infrastructure transition by quantifying the cost savings in reducing one workforce category (data center operators) as well as potential increased costs in other categories (cloud administrators, system administrators) depending on the specific service transition plan. An easy mistake to make in this example would be to calculate the potential benefit solely on a percentage decrease in employee count without considering the potential cost increase for retained or new workforce categories, which could result in actual benefits appearing lower than expected.

Cloud Computing Return on Investment

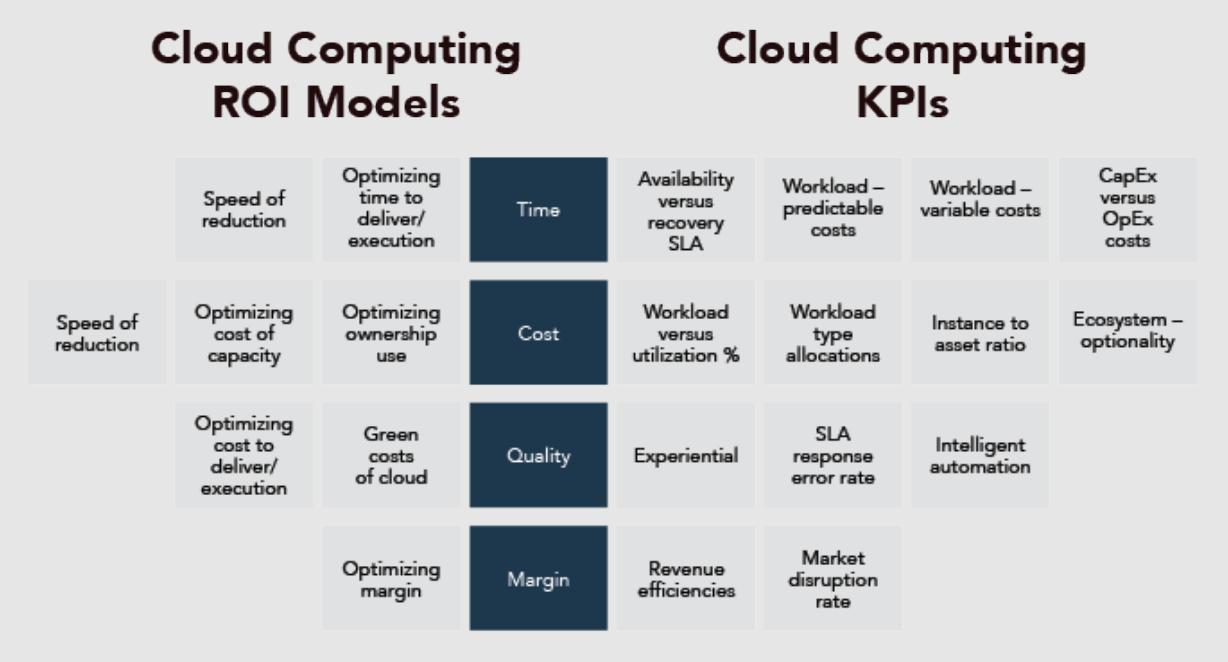


Figure 1.33: Cloud Computing Return on Investment Sample Model

Although business alignment is paramount, cloud-computing return on investment (ROI) must also be addressed. This metric should be addressed from multiple vantage points.

Cloud economic savings can be measured through the following key performance indicators (KPIs):

- Workload versus utilization percent
- Workload type allocations
- Instance to asset ratio
- Ecosystem optionality (increased flexibility to choose or change IT providers)

The ROI model can also include operational metrics, such as the speed of cost reduction, optimizing cost of capacity, and optimizing ownership use. Business value can also be gleaned from process time reductions, product quality improvements, and customer experience enhancements.

KPIs should have defined metrics based on either ISO 27004, relevant ISO publications, negotiated service-level agreements, or NIST Special Publication 800-55. Within each ROI domain, targeted values should address one of the following:

- Measures of effectiveness
- Measures of efficiency
- Impact measures

Functional Security Requirements

During due diligence activities connected to service aggregation, it is imperative to consider capabilities that support **portability** and **interoperability**. After a determination of business requirements is made, deep research of CSPs may reveal that a selection of two or more providers is necessary. Proprietary nomenclature, methods and technologies espoused by the provider of choice could be potentially harmful to meeting the stated business requirements when it is necessary to link multiple services for a consuming organization.

ISO/IEC 19941:2017: Information technology—cloud computing—interoperability and portability focus on cloud service agreements related to interoperability and portability between cloud services. Interoperability extends the relationship between cloud and non-cloud services. The goal of interoperability is to provide seamless service consumption and management between standalone services and CSPs.

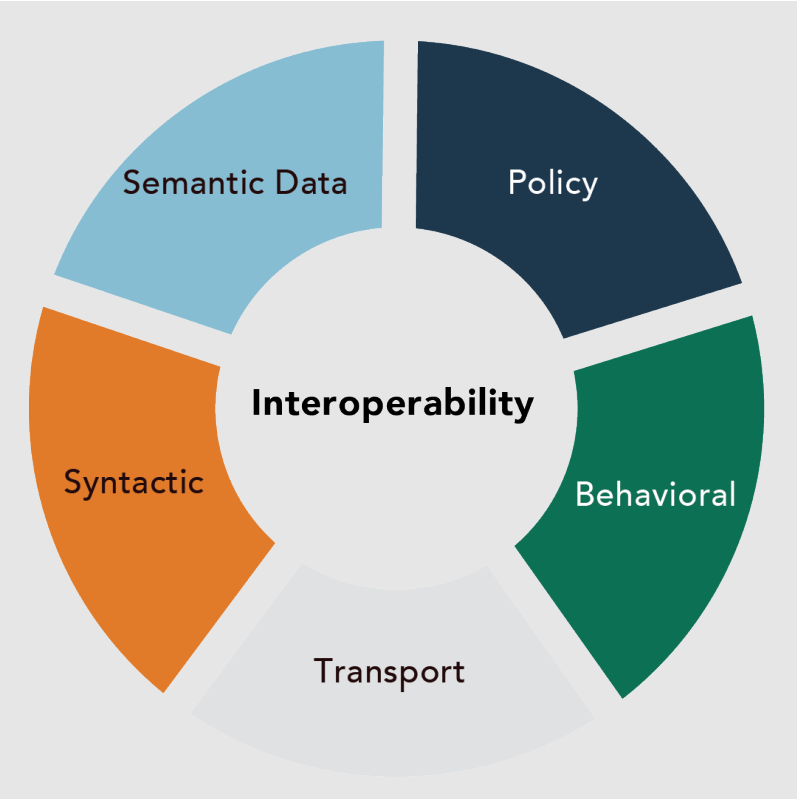


Figure 1.34: Cloud Interoperability

The five facets of cloud interoperability are:

- Policy
  - When two or more systems interoperate while complying with governmental laws, regulations, and organizational mandates.
- Behavioral
  - When the results of the use of exchanged information match the expected outcome.
- Transport
  - Commonality of the communication between cloud consumer and provider and other providers (e.g., http/s and various message queuing standards).
- Syntactic

    - When two or more systems understand the other systems' structure of exchanging information through encoding syntaxes (e.g., JavaScript Object Notation and XML).
- Semantic data
    - When systems exchange information to understand the meaning of the data model within the context (e.g., VMs, containers, storage and networking concepts).

The goal of portability is to enable cloud service customers to move their data or applications between standalone services and CSPs.

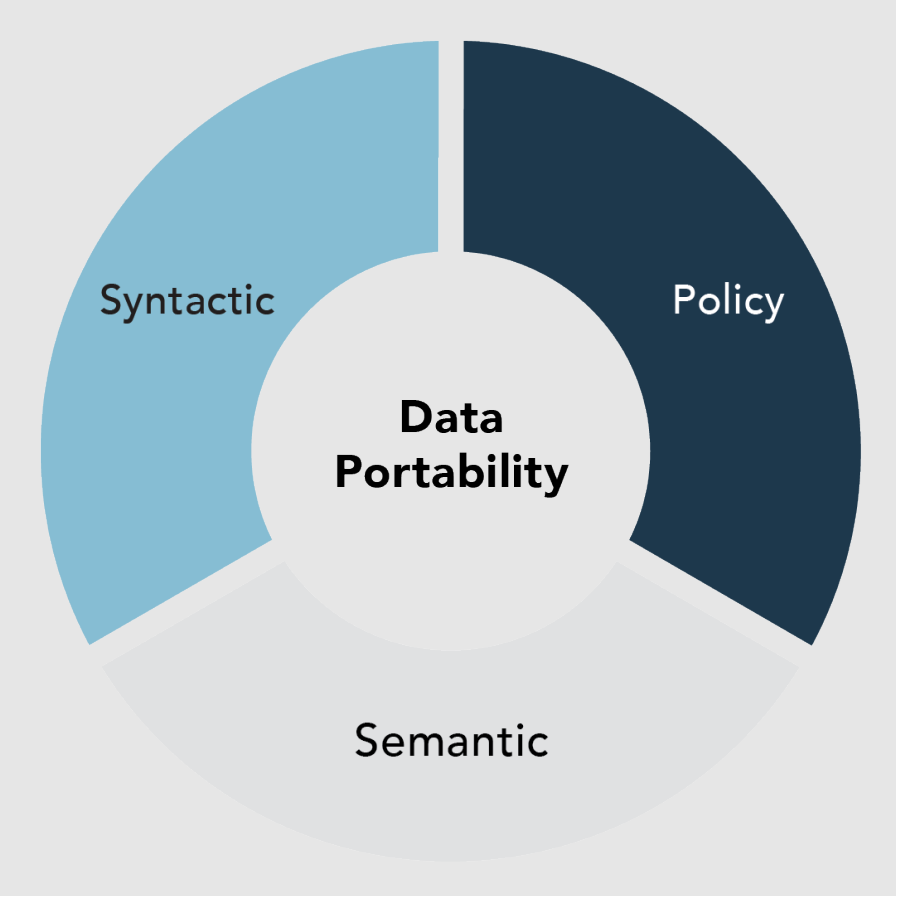


Figure 1.35: Cloud Data Portability

The three facets of cloud data portability are:

- Syntactic
  - Transferring data from a source system to a target system using formats that can be decoded on the target system with such features as XML or Open Virtualization Format (OVF)
- Semantic
  - Transferring data from a source system to a target system so that the data model is understood within the context of the subject area by the target
- Policy
  - Transferring data from a source system to a target system so that governmental laws, regulations and organizational mandates are followed

Security Considerations for IaaS, PaaS, and SaaS

As noted in Domain 1.3, many of the same security issues and threats that affect any IT system will also potentially impact a cloud-based capability. Depending on the cloud services chosen as part of the overall architecture and based on the areas of shared security responsibilities within a particular cloud-based capability set, specific security considerations can vary widely. Many of the potential security considerations will be covered in later domains, and the summary of common areas for security consideration are included here. This list is not comprehensive, and not all may be equally important to every cloud design. It is up to the CCSP to determine the applicability and potential impact of security risks to implementation.

Here are a few common security considerations for design and implementation of cloud-based capabilities. Depending on the specific service implementation and where the service falls within the shared security model, these security considerations may be of concern for the CSP, cloud consumer or both:

- *Virtual machine attacks.* Active VMs are vulnerable to all traditional attacks that can affect physical servers. Once a VM is compromised, it may be able to attack other VMs running on the same physical host because the VMs share

the same hardware and software resources. In addition, the compromised VM may be able to attack other VMs and hosts throughout the LAN.

- *Virtual network.* The virtual network contains virtual switch software that controls the movement of traffic between the virtual network interface cards (NICs) of the VMs and the physical NICs of the host. Virtual networks can be improperly configured or implemented by either the cloud customer or provider.
- *Hypervisor attacks.* Compromising the hypervisor enables the hacker to gain control over the VMs as well as the host. One example of a hypervisor attack is hyperjacking, which involves installing a rogue hypervisor that can take complete control of a host. This may be accomplished using a VM-based rootkit that attacks the original hypervisor, inserting a modified rogue hypervisor in its place.
- *Software and platform maintenance.* As with any IT capability, software and system components must be maintained and patched. This includes maintenance and monitoring of configurations, but also includes patching and updating components. Depending on the set of services or capabilities chosen for a solution, it is likely that the CSP will maintain some components while the cloud customer may be required to maintain others. The exact distribution of responsibility must be analyzed to ensure there are no maintenance gaps where neither the provider nor customer are maintaining a component.
- *Denial-of-service (DoS) attacks.* These attacks can be against internal components (e.g., attempting to cause runaway resource consumption that impacts operation) or against access (e.g., attaching interfaces or networks). While many cloud services include significant protections against some types of DoS attacks, they can still be vulnerable to others. For example, a cloud service may be protected from a typical network-based Distributed DoS (DDoS) attack against the network infrastructure due to the distributed nature of the cloud data centers and availability zones, however, the client application running on a service may still have interface limitations (e.g., concurrent connections limits) and might still be susceptible to a targeted denial-of-service attack.
- *Multitenancy.* Different users within a cloud share the same applications and the physical hardware to run their VMs. This sharing can enable information

leakage exploitation and increase the attack surface and the risk of VM-to-VM or VM-to-hypervisor compromise.

- *Workload complexity.* Server aggregation increases the amount of workload and network traffic that runs inside the cloud physical servers, which increases the complexity of managing the cloud workload.
- *Loss of control over data residency.* Users are not aware of the location of their data and services, and the cloud providers running VMs are not aware of their contents.
- *IAM.* IAM enables users to access IT services, resources, data and other assets. Access management helps to protect the confidentiality, integrity and availability of these assets and resources, ensuring that only those authorized to use or access them are permitted. Within the cloud infrastructure, it may be necessary to properly implement IAM at multiple levels. This can include IAM for access to the cloud (e.g., access to the **cloud management** console), IAM for potentially multiple infrastructure services (e.g., Windows or Linux VMs running in an IaaS or IAM for access to PaaS services from the CSP) or IAM for application access, which could include cloud customer applications in IaaS, PaaS or the CSP-operated SaaS where the cloud customer is still required to define levels of access for individual users.
- *Data Access Policies.* Customer policies for access to data must still exist for the cloud and must be implemented at all relevant levels of cloud technologies. For example, if a regulatory requirement exists for a legal jurisdiction, the cloud customer should have a policy that describes how the organization will comply. That policy must be consistent and cover the necessary elements to allow system administrators or cloud designers to develop solutions in accordance with the policy. If the policy disallows external entity access to data, then simply placing that data in an unencrypted form within a cloud infrastructure may not be possible since the CSP would have access to the data. Designing a solution that protects against the exposure of sensitive data to the CSP would require careful application of cryptographic functions and key management outside the CSP and could limit the utility of moving the data to the cloud in the first place. As such, this issue needs to be addressed as part of the initial design and may not be a technical issue at all in many cases.

Cloud Design Patterns

Design patterns can be best described as a standardized or "known good" way of implementing some capability. This can range from a standardized block of code implementing an application interface to standardized configurations for an operating system. To be considered known good, the design pattern will typically have been implemented in one or more specific cases and tested or evaluated over time to provide an elevated level of assurance that the design pattern is effective. This does not guarantee that any design pattern is perfect or that it would be good for all potential use cases. It does, however, provide a level of standardization and make misconfiguration or errors less likely while generating some level of confidence in the quality of the design. The specific level of confidence may depend on the rigor involved in the testing of the design pattern, how long or how widely previous implementations have been deployed, and whether a particular use of the pattern is identical or similar to previously tested uses of the pattern. Any of these factors can increase or decrease the confidence level that a design pattern will provide the expected results.

A cloud design pattern extends the concept of design patterns to cloud implementations. This can be particularly valuable in cloud design where improper implementation or misconfigurations can have significant impact. It can also simplify installation, maintenance and monitoring of cloud services when common cloud design patterns are consistently used.

While the use of secure cloud design patterns will never guarantee security or even guarantee future effectiveness of security objectives, they can significantly reduce risks associated with misconfigurations as well as limit the unique implementations of cloud services that make monitoring status or evaluating security difficult over time.

Well-Architected Framework

Each CSP has its own well-architected documents. It must be remembered that these are written by the CSPs to drive additional workloads to their solutions. For consumers, however, these may not be the best solutions. Generally, CSPs attempt to provide good advice to consumers to help them get the best from the CSP environment. An understanding of the applicable framework will provide a

common language in which to discuss requirements and design appropriate solutions. The context here is that the well-architected frameworks are designed to align the consumer's choices with the best practices for the target cloud, while keeping the CSP in the role of processor. However, the consumer remains accountable at all times for ensuring that everything done, either by themselves or on their behalf, is in line with their requirements.

The well-architected documents talk in terms of the pillars and principles that their respective frameworks are built on. The CSPs provide many self-assessment tools that a consumer can use to determine how closely their architecture conforms to these principles. The CSPs encourage consultancy firms to partner with them to provide onboarding advice to consumers. These consultancies develop well-architected landing zones—infrastructure that is built, prior to workloads being migrated. The landing zones' suitability to the workloads they will support have a major effect on the pace and success of the migration. Landing zones work well for applications conceived and designed for cloud deployment.

A well-architected landing zone cannot, however, fix an application that only scales vertically. It is larger servers that allow such an application to scale.

The fine details of the well-architected framework vary between CSPs. Here are the general principles, leaving the details to each CSP's own documentation.

At the highest level, a well-architected framework covers:

- *Operational excellence.* This includes the running and monitoring of systems. Activities supporting this are automating changes, defining standards, responding to events and continuous improvement.
- *Security.* This covers managing the confidentiality and integrity of data. Activities include managing user permissions and establishing controls to detect and analyze security events.
- *Reliability.* The availability of workloads and recovery from failures are included in this general principle. The activities are designed for availability with multiple availability zones, highly available instances and BCP DR.
- *Performance optimization.* This principle incorporates selecting resource types that are rightsized to workloads. Activities include the monitoring and reporting of under- and over-utilized resources.

- *Cost optimization.* The goal is to avoid unnecessary costs. Activities include understanding spending across accounts, selecting resources of the right type and quantity and balancing the scaling-out demands with associated costs.
- *Sustainability.* This encompasses green IT. Activities include looking at how the CSP measures and discloses its carbon footprint, how the customer contributes to it, and how it can reduce its carbon footprint.

DevOps/DevSecOps

DevOps is often described as a logical extension of Agile, pioneered by lean-thinking organizations seeking solutions for rapid and frequent delivery of software. Organizations have adopted DevOps and continue to do so, for a variety of reasons—most notably because of deficiencies in legacy IT practices, resulting in their inability to deal with how code change velocity has increased due to business needs.

Technological aspects of DevOps are primarily about continuous integration/continuous delivery (CI/CD) practices, relying on the automation of much of the routine work of transforming code changes into working software, including delivering tested code into production.

Tools and technologies have been introduced for this specific purpose, but successful implementation of DevOps requires special attention to—and organizational investment in—people and processes in addition to technology.

DevSecOps concerns bridging the gap between security and DevOps. Security should remain focused on minimizing enterprise risk and at the same time allow development to deliver more secure code at DevOps speed. This implies that traditional resource-intensive and heavyweight security activities and controls at various touchpoints throughout the software development life cycle must change to allow for the adaptation of principles that have proven successful for DevOps. As depicted in the figure below, security must be injected into the existing development workflow in the DevOps life cycle.

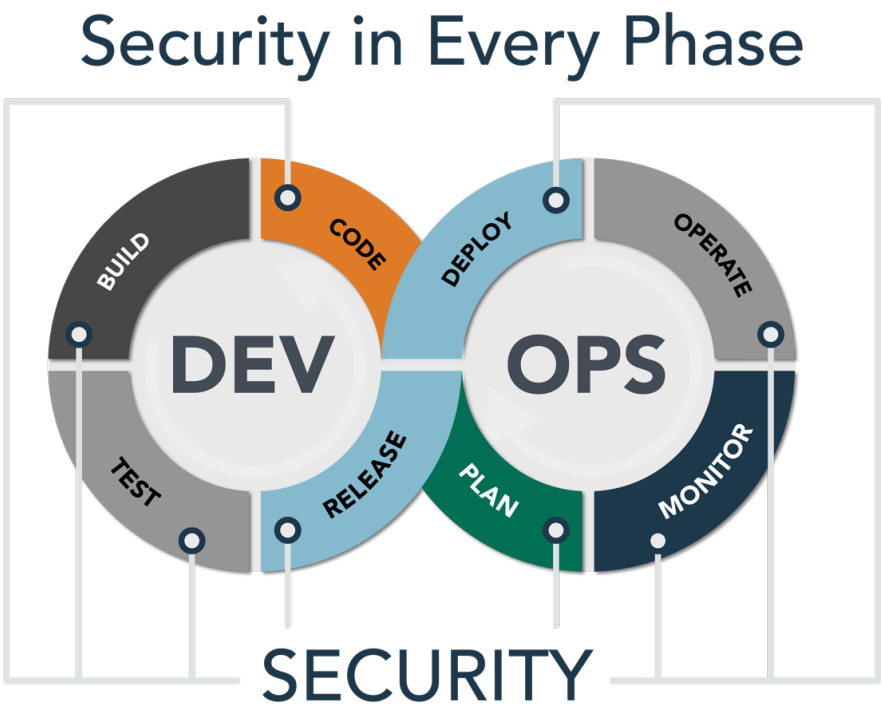


Figure 1.36: Security in Every Phase

Continuous Integration/Continuous Deployment

DevOps requires tasks such as builds, testing and deployment to occur frequently and naturally. For that to happen, such tasks must be automated. CI/CD practice relies on the automation of much of the routine work of transforming code changes into working software, including delivering tested code into production.

Continuous integration is a reference to the build and test cycle. Continuous integration (CI) servers build the project from scratch when developers merge changes into a shared version control repository. CD refers to the code movement from one environment to another (e.g., dev to QA to UAT). CI and CD typically go hand in hand and the same CI server will likely also handle CD.

In practice, CI/CD would rely on a system to trigger the process of compilation and run all tests and checks that have been automated. With this practice, every change that passes all stages of the production pipeline is released to customers with no human intervention and only a failed test will prevent a new change from being deployed to production.

Evaluate Cloud Service Providers (1.5)

Objective

- Analyze key cloud service providers and identify the potential tools, frameworks and registries that evaluate them.

Overview

There are thousands of cloud service providers in the marketplace, with hundreds being added every day.

Cloud computing introduces a dynamic and fluid boundary between a cloud-consuming organization and a cloud provider. Historically, IT was either owned and operated by the consuming organization or managed in a dedicated way by an external provider.

The cloud-essential characteristics directly affect this boundary and make it more dynamic and fluid. On-demand self-service blurs the line between who is responsible for the management of specific processes and controls, the customer or provider.

Evaluating Cloud Service Vendors

A cloud consumer should evaluate the options available to them from a variety of different cloud vendors/providers before selecting a vendor or specific cloud service. In some cases, using multiple services from a single vendor may be more attractive, while in other cases, selecting services from different vendors/providers may be advantageous. Regardless, the consumer should carefully weigh the advantages and disadvantages of each potential approach. A consumer might consider how vendors compare in terms of functional services, compliance to standards or frameworks, or suitability of standard (or negotiable) terms and conditions. A consumer might also consider the level of effort and technical expertise required to implement, maintain and monitor a cloud service as part of the evaluation process.

A final overarching consideration may be over-reliance on a single vendor and the risks of vendor lock-in. It may be more cost effective and provide easier management in some cases to rely on a single Cloud Service Provider (CSP), but problems with that vendor, potential de-platforming concerns or risks related to vendor lock-in may make using multiple CSPs more attractive to some consumers. The final decision should be based on overall functionality, a realistic estimate of total costs (service costs plus maintenance and monitoring costs, personal costs and other indirect costs for development or other maintenance activities), and a risk assessment of chosen approach.

The following sections include some potential tools, frameworks and registries that can help consumers research and determine risks associated with CSPs. In many cases, the CSP will provide a significant amount of information on compliance with standards and certifications on the website for the potential consumer. However, it is often advantageous to compare multiple providers using the same compliance frameworks or standards assessments.

Cloud Control Matrix (CCM)

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is a compilation of cloud-relevant security controls that can be related to other control frameworks. The CCM adapts security controls to a cloud-relevant format and includes consideration of shared security responsibilities between the cloud provider and consumer. The CCM is designed to be used with the Cloud Assessments Initiative Questionnaire (CAIQ), with the CAIQ being either distributed by the provider to customers or potential customers, or publicly posted in the STAR registry. Together, the CCM and CAIQ provide a significant amount of security-relevant information on the cloud provider's capabilities and security controls. They will also identify customer responsibilities, which helps customers understand the security tasks or controls that they must perform to ensure there is no security control gap.

CSA Security, Trust Assurance and Risk (STAR) Registry

Cloud Security Alliance's Security, Trust Assurance and Risk (STAR) registry provides a mechanism to assist consumers in comparing and evaluating cloud service providers. The registry allows CSPs to self-assess or to seek different types of third-party assessment against standardized controls. The STAR Level 1 registry

includes providers that have conducted a self-assessment, while the STAR Level 2 registry includes providers that have obtained one of several forms of third-party audits. The STAR Level 3 registry has not been released but will include some type of continous or ongoing monitoring of the cloud service provider.

CSA STAR Level 1: Self-Assessment

Typically, organizations operating in low-risk environments that want to improve trust and transparency pursue Level 1. The Level 1 self-assessment requires that a service provider self-assess against the Cloud Controls Matrix (CCM), which offers a listing of applicable cloud relevant security controls. Generally, cloud providers complete the Cloud Assessments Initiative Questionnaire, which is submitted to the STAR registry. The CAIQ documents security control compliance and is included in the public domain Level 1 registry.

Additionally, service providers may opt to complete a CSA General Data Protection Regulation (GDPR) assessment for the services they provide. This is often referred to as GDPR Code of Conduct (CoC) and includes two documents: Code of Conduct Statement of Adherence and PLA Code of Practice (CoP) Template. Compliance with Registry attestation is valid for 1 year

CSA STAR Level 2: Third-Party Certification

Typically, organizations pursue Level 2 when operating in a medium to high-risk environment. To achieve Level 2, a provider must undergo a third-party audit. The CSA supports integrating the CCM audit with ISO 27001 (STAR Certification) and a SOC 2 Type 2 (STAR Attestation). CSA maintains a list of authorized auditors to support this process. For organizations operating under the guidance of SOC Level 2 can also be obtained for China using the CSA C-STAR assessment. The CCM audit when combined with the ISO 27001 or SOC 2 Type 2 makes the audit more relevant to the cloud. Generally, organizations achieve and maintain ISO27001, SOC 2, GB/T 22080-2008, or GDPR prior to achieving STAR Level 2.

CSA STAR Level 3: Full Cloud Assurance and Transparency

A third level (Level 3) has been proposed but has not been released as of Q1 2022. Initial proposals for Level 3 included consideration for some type of continuous or ongoing monitoring of the CSP.

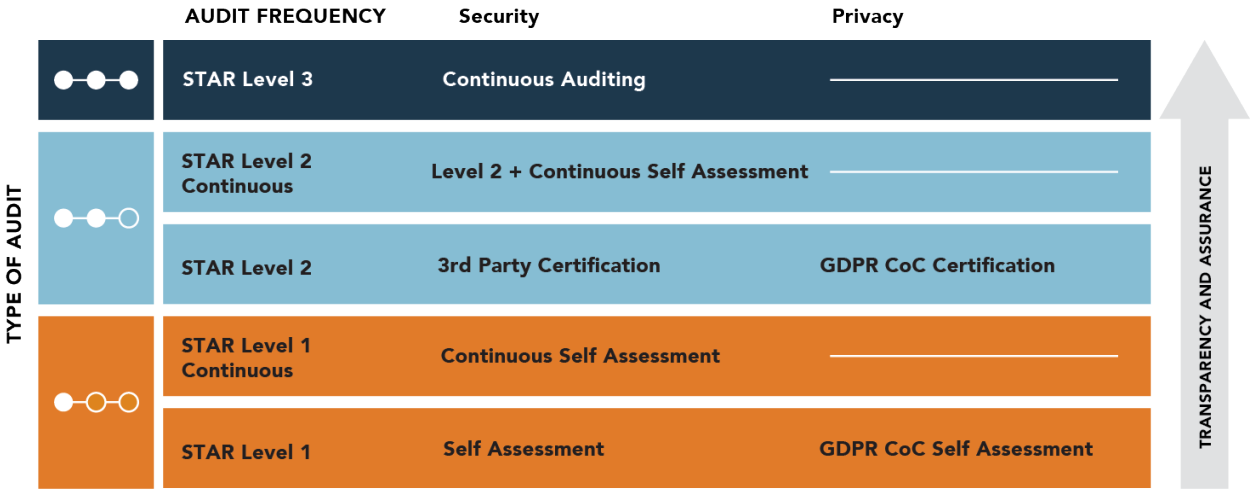


Figure 1.37: STAR Level

Other Cloud Audit Programs

Numerous other audit programs are applicable to the cloud. Some are relevant to industries or use cases (e.g., HITRUST CSF, PCI), some apply to regions (e.g., EuroCloud STARAudit) and some are specific to certain governments (e.g., ISMAP-Japan, FedRAMP-USA, IRAP-Australia, etc.). Many larger CSPs that operate globally will obtain and maintain multiple certifications across geographic regions and industries; however, it is always the cloud consumer's responsibility to assess each provider service to ensure it meets the standards or compliance requirements for the customer's intended use of the service.

One issue with many cloud providers is that they will not always have the same level of compliance for every service they provide. In many cases, compliance and audits are conducted for individual services. This can result in a particular cloud service from a CSP being compliant to a consumer need while another service from the same CSP is not.

Verification Against Criteria

It is always the cloud customer's responsibility to determine what requirements must be met by a cloud service or cloud provider and to ensure the providers they choose or utilize meet those requirements.

Cloud consumers should always consider their requirements before transitioning any capability to a cloud service and should also periodically review existing cloud services to ensure they continue to meet requirements. CSPs may periodically change technical elements of their provided services, and in some cases will change acceptable use policies, terms and conditions or service-level agreements so that a service that previously met customer requirements will no longer meet those requirements.

Later domains will discuss the execution of a gap analysis and other techniques that can be used to verify that a service meets a customer's criteria. The overarching concern is that a cloud service or capability meets a set of well-defined customer criteria and is periodically reviewed.

Besides verification of technical capability, which will be covered more in later domains, the following items should be verified against customer requirements from the legal, contractual and overall service level provisioning perspective.

ISO/IEC 27017:2015

ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

- Additional implementation guidance for relevant controls specified in ISO/IEC 27002
- Additional controls with implementation guidance that specifically relate to cloud services

This standard provides enhanced controls for cloud service providers and cloud service customers and should be used in conjunction with the ISO/IEC 27001 standards series. By clarifying both parties' roles and responsibilities, it is intended to assist in making the safety and security of cloud services equivalent to other certified information management systems.

The standard not only provides guidance on ISO/IEC 27002 security controls, but it also introduces seven new cloud-specific controls. These enhancements address:

- Delineation of responsibilities between the cloud service provider and cloud customer
- Disposition of assets upon contract termination
- Cloud service customer virtual environment protection and isolation
- Virtual machine configuration
- CSP cloud environment administrative operations and procedures
- Cloud customer monitoring of activity within the cloud
- Virtual and cloud network environment alignment

Payment Card Industry Data Security Standard (PCI DSS)

The **Payment Card Industry Data Security Standard** (PCI DSS) is a requirement administered by the Payment Card Industry Security Standards Council. It is mandated by credit card brands to establish proper control of cardholder data and reduce potential fraud. PCI DSS is covered in more detail in Domain 6.3.

System/Subsystem Product Certifications

Various certifications exist to support the technical evaluation of products and services. These can be used by an organization to help determine what is or is not being effectively done by the product or service. Certification does not guarantee security for any particular use case; it only identifies system capabilities with a level of confidence. Two examples are provided: the international Common Criteria program under ISO 15408 and the United States FIPS 140-2/3 program for cryptography.

Common Criteria

The Common Criteria is an international set of guidelines and specifications (ISO/IEC 15408) developed for evaluating information security products to ensure they meet an agreed-upon security standard for government entities and agencies. Until 2005, this standard was known as The Trusted Computer System Evaluation Criteria.

The Common Criteria has four key components:

- *Protection profiles (PP).* A protection profile defines a standard set of security requirements for a specific type of product, such as a firewall, IDS or unified threat management (UTM).
- *Target of evaluation (ToE).* The vendor product is examined against this specific profile by a third-party evaluation lab using a common evaluation methodology (CEM).
- *Security target (ST).* An overview, provided by the vendor, of the product and product's security features, an evaluation of potential security threats, and the vendor's self-assessment detailing how the product conforms to the relevant protection profile.
- *Evaluation assurance levels (EALs).* This defines how thoroughly the product is tested.

Evaluation assurance levels are rated using a sliding scale from one to seven, with one being the lowest-level evaluation and seven being the highest. The higher the level of evaluation, the more quality assurance (QA) tests it has undergone. This does not necessarily mean more secure, however.

- EAL1: Functionally tested
- EAL2: Structurally tested
- EAL3: Methodically tested and checked
- EAL4: Methodically designed, tested and reviewed
- EAL5: Semiformally designed and tested
- EAL6: Semiformally verified design and tested
- EAL7: Formally verified design and tested

Criteria Evaluation Process

The goal of Common Criteria certification is to assure customers that the products they are buying have been evaluated and that a vendor-neutral third party has verified the vendor's claims.

To submit a product for evaluation:

- The vendor must first complete a security target (ST) description, which includes an overview of the product and product's security features, an evaluation of potential security threats, and the vendor's self-assessment detailing how the product conforms to the relevant protection profile at the evaluation assurance level the vendor chooses to test against.
- The laboratory (which must comply with ISO/IEC 17025) then tests the product to verify the product's security features and evaluates how well it meets the specifications defined in the protection profile.
- The results of a successful evaluation form the basis for an official certification of the product.

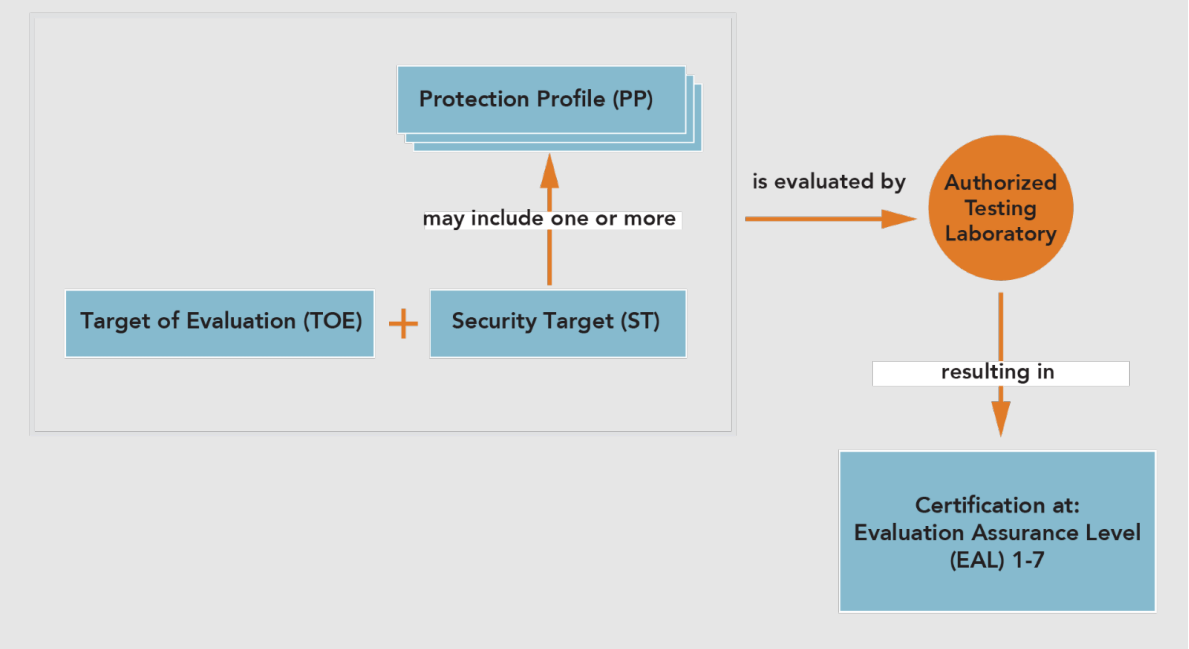


Figure 1.38: Common Criteria

Note that Common Criteria looks at certifying a product only and does not include administrative or business processes. The negative aspects of Common Criteria include that it may take more than one year to test a product, the process is expensive, and the vendor may have improved the product since it was submitted for testing.

FIPS

To be FIPS compliant, an organization must adhere to the standards outlined in the Federal Information Processing Standards (FIPS). FIPS 140-2/3 is a product certification (they use the term validation) program to verify that a product meets a specific security standard. FIPS 140-2 and FIPS 140-3 compliant cryptographic modules are required for any use of cryptography that protects federal government data.

NIST programs validate cryptographic modules to ensure they are properly constructed and do not present flaws that could make cryptographic messages easier to break or compromise than the strength provided by the algorithm.

Specifies 4 levels (Level 1-4)

NIST supports with:

- Cryptographic Algorithm Validation Program (CAVP)
  - Validates algorithms are properly implemented
- Cryptographic Module Validation Program (CMVP)
  - Validates modules are properly implement and protect algorithms validated by the CAVP
- Testing by independent laboratories

FIPS 140-2 is in a multiyear transition and is being replaced by FIPS 140-3

- FIPS 140-3 Testing (CMVP) scheduled to begin Sep 22, 2020
- FIPS 140-2 Testing (CMVP) ends Sep 22, 2021
- FIPS 140-2 certificates expire Sep 22, 2026

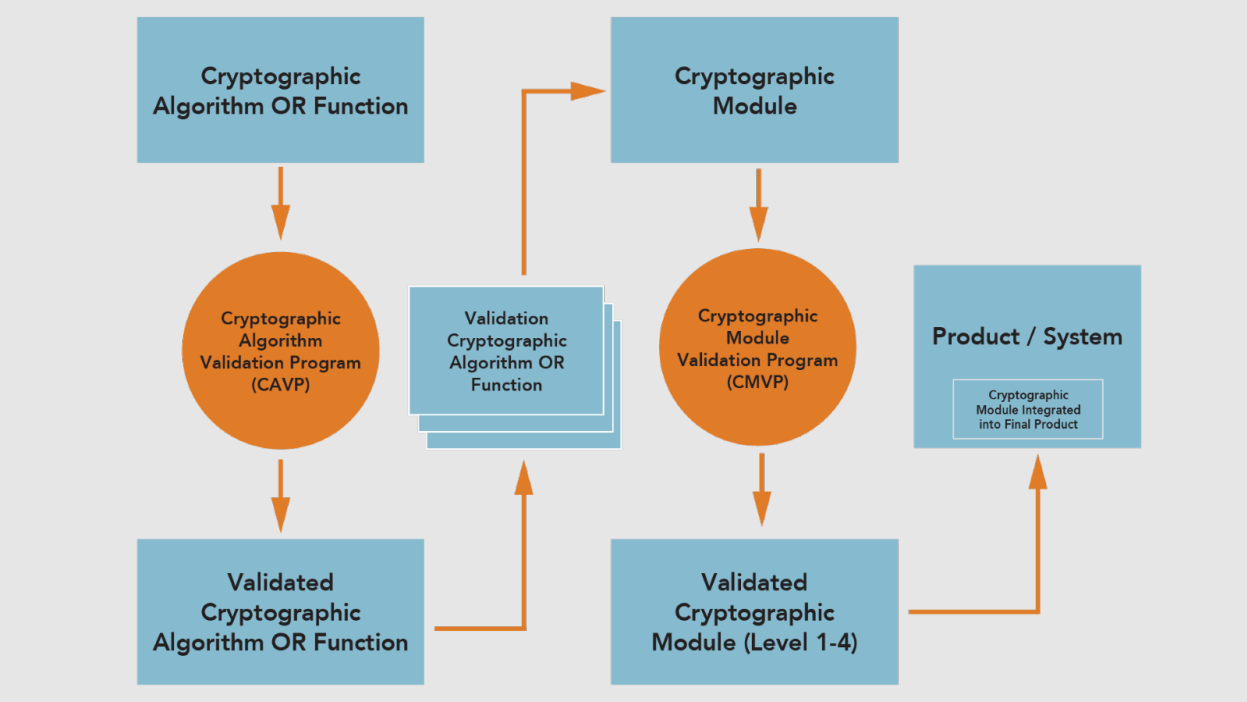


Figure 1.39: FIPS 140-2 Process

Summary

Cloud computing is not about technology. It is about consuming technology services in a manner that maximizes an organization's ability to attain the desired business or mission goals. Cloud computing is also about risk management. In managing risk, CCSPs must use their knowledge of how these services are best employed by understanding how each contributes to the mission or business model and how each protects confidentiality, integrity and availability of data within acceptable operational constraints. Domain 1 provides the foundational knowledge to be successful in that role.

Quiz

1. A company is intrigued with the potential cost savings from moving business processes to the cloud. One business process it seeks to move to the cloud is data storage. After reviewing the CSP's data-storage strategy, it is ascertained that it uses public cloud architecture. Which of the following answers provides the best solution to ensure the company's data is protected from other tenants?

   A. Use access control rules based on predefined business rules
   B. Require company data be kept in separate storage
   C. Ensure company data is encrypted
   D. Implement a hybrid cloud strategy using the CSP's application and storing the data locally

2. The second business process that the company wishes to migrate to the cloud is the human resources system. It has selected a SaaS cloud service model. When using a SaaS cloud service model, what tool is most effective at ensuring the security of a company's data?

   A. Ensuring all company data is encrypted before being loaded to the SaaS application
   B. Ensuring the company has the right to audit
   C. Defining the geographic restrictions of where the company's data is authorized to reside
   D. Reviewing the shared security model between CSP and consumer and ensuring that CSP and consumer responsibilities are met prior to using the service

3. Part of the company's risk management strategy is to ensure that security risk is properly addressed during migration to a cloud service provider.

Which of the following questions should not be considered during this process?

A. What negative consequences would the business encounter if the process was manipulated by an unauthorized person?
B. Would the business be impacted if the information became publicly available?
C. What is the total cost of security controls associated with moving the business process to the cloud?
D. If the process became unavailable, how would that affect the business?

4. The company has been running an existing e-commerce application on premises, which normally requires minimal resources. Periodically increased demand for resources that are not available to the system results in deficient performance and outages. The company wants to ensure it can support high-demand periods, such as holidays when resource demand increases quickly, without making a significant capital investment. Which concept would meet the business requirements?

A. Load balancing
B. Cloud bursting
C. High availability
D. Quad processors

5. Which deployment model best meets business requirements to retain full control over extremely sensitive data but minimize IT expenditures?

A. Private cloud
B. Community cloud
C. Hybrid cloud
D. Public cloud

6. In a SaaS service model, the tenant transfers technical control of the computing environment to the cloud service provider. Which of the following responsibilities does the tenant retain?

A. Configuration of the application
B. Backing up the data to a remote location
C. Patching the operating systems
D. Liability and legal responsibility for securing data

7. After researching the various cloud deployment models, the company decides that purchasing a dedicated cloud deployment model is not cost effective; however, it wants to ensure that all companies utilizing the cloud deployment model adhere to the same policy requirements. Which deployment model best meets these requirements?

A. Hybrid cloud
B. Community cloud
C. Private cloud
D. Public cloud

8. A startup company wants to become a SaaS provider. It intends to develop and sell the use of an application while minimizing staff requirements, as well as initial and ongoing expenditures. Which company service model best meets these requirements?

A. SaaS
B. IaaS
C. PaaS
D. On-premises

9. The company uses a custom application that services financial clients. The application is hosted on company servers within its confidential data center. All company servers run specific configurations and a software firewall. The company wants a test environment that offers control over the environment to assure configuration settings of both environments are alike but wants to minimize the costs and time involved with setting up the environment. Which service model best meets the business requirements?

A. SaaS / private
B. IaaS / public
C. PaaS / hybrid
D. IaaS / private

10. The company wants to move a business process to the cloud. The business process and associated data are heavily regulated. The company needs to ensure it retains ownership of the governing controls and has assurance the data will reside within a certain geographic location. Which deployment model best meets the business requirements?

A. Public cloud
B. Private cloud
C. Hybrid cloud
D. Community cloud

Quiz – Answers and Feedback

1. A company is intrigued with the potential cost savings from moving business processes to the cloud. One business process it seeks to move to the cloud is data storage. After reviewing the CSP's data-storage strategy, it is ascertained that it uses public cloud architecture. Which of the following answers provides the best solution to ensure the company's data is protected from other tenants?

A. Use access control rules based on predefined business rules
B. Require company data be kept in separate storage
C. **Ensure company data is encrypted**
D. Implement a hybrid cloud strategy using the CSP's application and storing the data locally.

Most CSPs offer encryption, which may be built into the storage service or may require cloud consumer action. If CSP-provided encryption is not available, the consumer may choose to employ their own encryption mechanisms. If the company data store was improperly exposed to another tenant, the data would remain confidential.

2. The second business process that the company wishes to migrate to the cloud is the human resources system. It has selected a SaaS cloud service model. When using a SaaS cloud service model, what tool is most effective at ensuring the security of a company's data?

A. Ensuring all company data is encrypted before being loaded to the SaaS application
B. Ensuring the company has the right to audit
C. Defining the geographic restrictions of where the company's data is authorized to reside
D. Reviewing the shared security model between CSP and consumer and ensuring that CSP and consumer responsibilities are met prior to using the service

Answer D is the most effective and the most likely to provide comprehensive security protections. It requires a review of the shared security model before using the service as well as the assurance that the service is properly implemented. Reviewing the CSP responsibilities may be available through review of third-party audits or other documentation, and properly configuring elements of the service within the scope of customer control is critical for employment of any cloud service.

3. Part of the company's risk management strategy is to ensure that security risk is properly addressed during migration to a cloud service provider.

Which of the following questions should not be considered during this process?

A. What negative consequences would the business encounter if the process was manipulated by an unauthorized person?
B. Would the business be impacted if the information became publicly available?
C. What is the total cost of security controls associated with moving the business process to the cloud?
D. If the process became unavailable, how would that affect the business?

While the scenario stated that the impetus for the company's cloud migration was cost savings, this question deals with risk. Part of determining whether processes or information are cloud ready is determining the impact of compromise to confidentiality, integrity, and availability. There should be a process for identifying the impact of each aspect of the CIA triad; this allows the business to determine the controls required to protect the information and whether costs of controls and potential impacts exceed the value of moving to the cloud.

4. The company has been running an existing e-commerce application on premises, which normally requires minimal resources. Periodically increased demand for resources that are not available to the system results in deficient performance and outages. The company wants to ensure it can support high-demand periods, such as holidays when resource demand increases quickly, without making a significant capital investment. Which concept would meet the business requirements?

A. Load balancing
B. Cloud bursting
C. High availability
D. Quad processors

Cloud bursting allows for public cloud resources to be utilized when a private cloud workload has reached maximum capacity. In this case, the existing on-premises infrastructure would work normally when resource use is within tolerance, but excess load to the system would be transferred to a cloud instance during peak or unusual demand.

5. Which deployment model best meets business requirements to retain full control over extremely sensitive data but minimize IT expenditures?

A. Private cloud
B. Community cloud
C. Hybrid cloud
D. Public cloud

The hybrid cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability. Utilizing a hybrid cloud, the organization can retain full control over a subset of their data (extremely sensitive) while leveraging a lower-cost public cloud for less sensitive data.

6. In a SaaS service model, the tenant transfers technical control of the computing environment to the cloud service provider. Which of the following responsibilities does the tenant retain?

A. Configuration of the application
B. Backing up the data to a remote location
C. Patching the operating systems
D. Liability and legal responsibility for securing data

As the data controller, the tenant retains all liability and legal responsibility for securing data.

7. After researching the various cloud deployment models, the company decides that purchasing a dedicated cloud deployment model is not cost effective; however, it wants to ensure that all companies utilizing the cloud deployment model adhere to the same policy requirements. Which deployment model best meets these requirements?

A. Hybrid cloud
B. Community cloud
C. Private cloud
D. Public cloud

The community cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations). It provides the benefits of a public cloud deployment, while maintaining heightened levels of privacy, security, and regulatory compliance.

8. A startup company wants to become a SaaS provider. It intends to develop and sell the use of an application while minimizing staff requirements, as well as initial and ongoing expenditures. Which company service model best meets these requirements?

A. SaaS
B. IaaS
C. **PaaS**
D. On-premises

PaaS provides the consumer with the capability to deploy onto the cloud infrastructure consumer-created or acquired applications using programming languages, libraries, services, and tools supported by the provider. This provides the startup company a platform to deploy its application and provide access to consumers in the form of a SaaS service model while minimizing staffing requirements.

9. The company uses a custom application that services financial clients. The application is hosted on company servers within its confidential data center. All company servers run specific configurations and a software firewall. The company wants a test environment that offers control over the environment to assure configuration settings of both environments are alike but wants to minimize the costs and time involved with setting up the environment. Which service model best meets the business requirements?

A. SaaS / private
B. **IaaS / public**
C. PaaS / hybrid
D. IaaS / private

IaaS in a public offering will provide the most control over the environment, ensuring configuration settings of the operating system, local software firewall settings, and applications in the cloud mirror the on-premises environment. Employing a public offering reduces the costs associated with setting up the environment, because the compute resources are shared among various organizations. No requirement to isolate the environment in a hybrid or private model was identified in the scenario. The capability to self-provision a new environment will occur quickly in a public/IaaS environment, making this a desirable approach.

10. The company wants to move a business process to the cloud. The business process and associated data are heavily regulated. The company needs to ensure it retains ownership of the governing controls and has assurance the data will reside within a certain geographic location. Which deployment model best meets the business requirements?

A. Public cloud
B. **Private cloud**
C. Hybrid cloud
D. Community cloud

Key drivers for a private cloud include ownership and retention of governance controls, assurance over data location, and removal of multiple-jurisdiction legal and compliance requirements.

Terms and Definitions

Authorization A method of determining whether a user should receive access to sensitive data or resources.
Authentication The act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information. Typically, a measure designed to protect against fraudulent transmissions by establishing the validity of a transmission, message, station or originator.
Business Continuity and Disaster Recovery The capability of an organization to continue delivery of products and services within acceptable time frames at predefined capacity relating to a disruption, along with the ability of the information and communication technology (ICT) elements of an organization to support its critical business functions to an acceptable level within a predetermined period following a disruption.
Cloud app (cloud application) A software application that is never installed on a local computer. Instead, it is accessed via the internet.
Cloud computing A type of computing that relies on sharing computing resources in the delivery of computing services, rather than having local servers or personal devices to handle applications.
Cloud computing role A set of activities that serves a common purpose. Common roles include cloud service customer, cloud service provider, and related sub-roles.

Cloud database A database accessible to clients from the cloud and delivered to users on demand via the internet. They can use cloud computing to achieve optimized scaling, high availability, multitenancy and effective resource allocation.
Cloud management Software and technologies designed for operating and monitoring the applications, data and services residing in the cloud. These tools help ensure a company's cloud computing–based resources are working optimally and properly interacting with users and other services.
Cloud migration The process of transitioning all or part of a company's data, applications and services from on-site premises behind the firewall to the cloud, where the information can be provided over the internet on an on-demand basis.
Cloud operating system (OS) A software application responsible for orchestrating cloud computing services across multiple geographically separated data centers.
Cloud service customer (CSC) A party that is in a business relationship for the purpose of using cloud services.
Cloud service provider (CSP) A service provider who offers customers storage or software solutions available via a public network, usually the internet.
Cloud storage The storage of data online in the cloud, wherein a company's data is stored in and accessible from multiple distributed and connected resources that make up a cloud.

Cloud workload The resources demanded by an application, service or capability running within the cloud environment.
Confidential computing A system that protects data in use by performing computation in a hardware-based Trusted Execution Environment.
Cryptographic key The input that controls the operation of the cryptographic algorithm. It determines the behavior of the algorithm and permits the reliable encryption and decryption of the message.
Cryptography The study or applications of methods to secure or protect the meaning and content of messages, files, or other information, usually by disguise, obscuration, or other transformations of that content and meaning. Used to secure information in the presence of adversaries.
Disaster Recovery as a Service (DRaaS) Service provided to on-premises data centers to recover to/from the cloud.
Ephemeral computing An approach with virtual systems or containerized applications where the system is designed not to require information or state to be maintained between operations. Also called nonpersistent computing.
Function as a Service (FaaS) A type of serverless technology that allows customers to develop, run, and manage application functionalities without the complexity of building and

maintaining the infrastructure typically associated with developing and launching an app. Typically used when building microservices applications.
Geofencing/geoblocking A technology that can relate a digital user to their actual physical location, or a close approximation thereof, and may be configured to take action based on a specific geographic boundary in the physical world.
Hybrid cloud A combination of public and private cloud storage where some critical data resides in the enterprise's private cloud while other data is stored and accessible from a public cloud storage provider.
Identity and Access Management Using multiple technologies and business processes to help the right people or machines to access the right assets at the right time for the right reasons, while preventing unauthorized access and fraud.
Infrastructure as a Service (IaaS) Typically, delivery of computer, storage, and networking services by ongoing contract or subscription. One example is a data center where software and servers are purchased as a fully outsourced service and billed according to usage.
Interoperability The ability of different information systems, devices, or applications to connect, in a coordinated manner, within and across organizational boundaries to access, exchange, and cooperatively use data.

Key management All processes used to create, store, distribute, and provide expiration and revocation of encryption and decryption keys, for all users of a particular encryption system.
Multitenancy Describes multiple customers using the same public cloud.
Network gateway A device or node that connects disparate networks by translating communications from one protocol to another.
Open Virtualization Format (OVF) A syntactic standard of sending and receiving data between different vendor virtualization systems.
Payment Card Industry Data Security Standard (PCI DSS) A requirement for vendors accepting credit card payments to establish proper control of cardholder data and reduce potential fraud.
Peer cloud service provider A cloud service provider who provides one or more cloud services for use by one or more other cloud service providers as part of their cloud services.
Platform as a Service (PaaS) A cloud service through which the customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more executing environments supported by the cloud service provider.

Portability When applied to cloud services, it defines the ease with which applications or components are moved and reused elsewhere regardless of the provider, platform, OS, infrastructure, location, storage, format of data, or APIs.
Private cloud The phrase used to describe a cloud computing platform that is implemented within the corporate firewall, under the control of the IT department.
Privileged Account Management (PAM) Refers to mechanisms that provide automated dynamic provisioning and deprovisioning of access on systems or services only when those permissions are required.
Privileged user management The process and ongoing requirements to manage the life cycle of user accounts with the highest privileges in a system.
Product catalog A listing of all the cloud service products that cloud service providers make available to cloud service customers.
Provisioning When applied to cloud services, the processes associated with delivering and orchestrating cloud computing services. It also includes facilities for interfacing with the cloud's applications and services as well as auditing and monitoring who accesses and utilizes the resources.

Routing tables A set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. Used by all IP-enabled devices, including routers and switches.
Software as a Service (SaaS) A software delivery method that provides access to software and its functions remotely as a web-based service. This allows organizations to access business functionality at a cost typically less than paying for licensed applications, since pricing is based on a monthly fee.
STAR Registry (Cloud Security Alliance's Security, Trust Assurance and Risk registry) A mechanism to assist consumers in comparing and evaluating cloud service providers.
Sub-role A subset of the activities of a given role.
Virtual machine A system that allows multiple virtual systems to share a common physical implementation.
Virtual private cloud A logically isolated section of a cloud where resources can be launched in a virtual network that is customer defined. The customer has complete control over their virtual networking environment, including selection of private IP address range, creation of subnets, and configuration of route tables and network gateways.

Key Takeaways

Understand Cloud Computing Concepts (1.1)

CCSPs must put definitions of cloud-computing terms, descriptions of the characteristics of the cloud, and roles that support a cloud service into practice. After understanding the formal definitions and the types of cloud computing that are available, Cloud Service Provider (CSP) offerings can be compared to these formal definitions to create a gap analysis. This analysis will allow exploration of any mismatch between formal definitions and the offered service.

Cloud computing roles are defined for both customer and service provider, but the issue of who performs each of the roles is less important than understanding whether all roles are covered. If a role is not covered, there will be a gap in service and potentially a gap in security.

The characteristics of cloud computing require CCSPs to look at what is offered by the supplier and assess whether all characteristics are available. If they are not, the service is not a true cloud service. It may provide value, but it must be assessed as a managed service.

All the financial benefits of cloud computing will not be delivered if all the cloud characteristics are not in place. The essential characteristics of cloud computing are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

Building blocks – computing, storage, and networking services – must be reviewed when assessing a cloud service. The security of the service depends on the design and implementation of these building blocks. If these foundations are not in place, the security of the cloud offering will be compromised.

Describe Cloud Reference Architecture (1.2)

A reference architecture comprises a set of patterns, lists, and descriptions that are accepted as best practice. Selecting the right cloud option is a complex task, and

reference architectures help CCSPs understand the nature of what a cloud service should be at an abstract level. These architectures are powerful tools in both cloud design and vendor assessment.

When examining cloud solutions:

- The provider has responsibility for security of the cloud.
- The customer has responsibility for security in the cloud.

Viewing security as a shared responsibility requires that services are analyzed to ensure that every component is being maintained by either the provider or the customer.

The two architectures covered are most widely used by organizations to design and assess cloud services and infrastructure:

- NIST Cloud Computing Reference Architecture and Taxonomy
- ISO/IEC 17789 Cloud Computing Reference Architecture (CCRA)

When assessing the security of a vendor's cloud architecture, compare the commercial offering with the reference and note any gaps as action points to be addressed.

Note that commercial offerings may differ from standard definitions. The CCSP must assess these variations, in the context of the organization's mission, to decide whether they enhance or detract from the required service capability or the security of that service.

Formal definitions of public, private, hybrid, and community cloud services are written from a vendor-neutral perspective. Every cloud provider's product literature will not employ the same terminology, and their sales staff may not comprehend cloud computing in the formal context that you have come to understand.

Always look for evidence that the service that is offered truly matches organizational needs. Included in this assessment should be a comparison with formal definitions. This will assist in comparing competing offers to find the best fit for each use case.

The cloud provides the opportunity for consumers to quickly try or adopt different technologies as they emerge and become available, such as related technologies like machine learning and artificial intelligence. This is a good example of how the cloud can provide advantages: to run proof-of-concepts and experiments very quickly and with low commercial outlay. This reduction in time-to-market is one of the greatest commercial benefits of cloud computing and one which sets it apart from traditional data center computing.

Understand Security Concepts Relevant to Cloud Computing (1.3)

Cryptography and key management are only defined in Domain 1, but it is critical at this stage to recognize that only very well-tested and publicly accepted cryptography solutions should be utilized and that only experts should write cryptographic functions. Content about security design and application (specifically in Domains 2 and 5) provides guidance for which type of cryptography to apply to a particular problem.

Media sanitization addresses information required to clean cloud systems of data that has been processed on the cloud before they are returned to the cloud provider. Cloud providers excel at providing information on their processes for destroying all data when equipment reaches its end-of-life. However, since most CCSPs work in a multi-tenanted environment (unless utilizing a private cloud), assurance that any data on the cloud provider's hardware is sanitized before the hardware is made available to another tenant is necessary. Acquiring this information about how data is sanitized before hardware delivery to another client can be challenging. When selecting a CSP, determine the necessary level of assurance and search the market for a solution that meets those needs.

Regarding the shared responsibility model of cloud computing, consider which parts of cloud security will be the responsibility of the consumer. CSPs provide a base set of services, but they will require additions to meet an organization's specific requirements. For example, security for virtualization (such as container security and network security) requires significant configuration by the consumer using the tools provided by the vendor. It is the responsibility of the consumer to augment these tools as required, possibly with tools from other vendors.

CCSPs may wish to implement a zero trust model, and many vendors will discuss their ability to put zero trust in place for an organization. However, only internal security professionals will understand the boundaries of trust within their organization, how they are mapped onto business processes, and how they can eventually be mapped onto computing, storage, and networking services. The implementation of zero trust is therefore mostly a consumer activity.

Designs should illustrate where the boundaries of trust must be drawn to support zero trust. Trust nothing, verify everything, and disallow anything not explicitly allowed. These are the basics of zero trust networking.

Understand the Design Principles of Secure Cloud Computing (1.4)

The secure data life cycle is only defined in Domain 1 and will be reviewed as a cloud data concept in Domain 2. As a design principle, ensure that a CSP's ability to provide services that underpin the secure data life cycle is tested at a level of assurance that meets organizational requirements.

Disaster Recovery is an area where cloud computing can deliver huge cost savings compared to physical data centers. Examine the options in Domain 1 and Domain 3 carefully to identify potential economic benefits and increased resiliency for organizations.

In addition to considerations of cloud characteristics and portability, build functional security requirements against the expected characteristics of a cloud service. Test these requirements against offerings from cloud vendors.

When assessing offers from a range of suppliers, it is useful to have a set of must-have requirements in addition to the cost-benefit analysis. This may help eliminate vendors early in the selection phase, saving time for both CSC and CSP.

Remember that not all business functions will fit into every cloud service model or deployment model. Identified requirements will guide which sections of an organization are best served by specific service and deployment models; this will inform designs and potential vendor lists.

Evaluate Cloud Service Providers (1.5)

Verification Against Criteria

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27017
- Payment Card Industry Data Security Standard (PCI DSS)

System/subsystem Product Certifications

- Common Criteria (CC)
- Federal Information Processing Standard (FIPS) 140-2

When evaluating cloud services, CCSPs should identify whether there is a community of customers similar to their organization with a common set of certification requirements and look for a CSP who addresses that specific community. If a community solution is unavailable, review requirements and share them with the cloud service provider.

Building almost anything with the cloud is possible, but that does not mean that every cloud solution is the best starting place to meet regulatory requirements. Vendor certifications should be assessed for their utility against organizational assurance requirements to reduce the burden on the consumer and the supplier. Technology can be outsourced, but accountability cannot. Forcefully challenge the contribution that a cloud service provider can make to any regulatory requirement. Treat each certification as a building block in assessment of the CSP and test the scope of each certification against specific use cases.

Assessment processes:

Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

- This is a compilation of cloud-relevant security controls that can be related to other control frameworks.
- CSPs can publish the results of their assessments on the CSA's Security, Trust Assurance, and Risk (STAR) Registry. These can be either self-assessed or assessed by a third party.

ISO/IEC 27017:2015

- This provides guidelines for information security controls that apply to the provision and use of cloud services and can be used in conjunction with the ISO/IEC 27001 certification.
- ISO/IEC 27001 audit is performed against a 'Scope of Attestation' that accompanies the certificate, but CCSPs may also want to see the whole audit report. (NIST special publications will be of interest to the CCSP, and SP800-53 has similar goals to ISO-2700X).

The Payment Card Industry Data Security Standard (PCI DSS)

- This is a requirement administered by the Payment Card Industry Security Standards Council and is mandated by most credit card brands.

ISO/IEC 15408 Common Criteria

- These are an international set of guidelines and specifications developed for evaluating information security products to ensure that they meet an agreed-upon security standard for government entities and agencies.

FIPS

- This acronym refers to Federal Information Processing Standards.
- FIPS 140-2 and FIPS 140-3 describe assurance for compliant cryptographic modules required for any use of cryptography that protects US federal government data.
- They provide information that could be useful for any CCSP who is defining cryptographic standards for their organization or assessing cloud services.

It is always the cloud customer's responsibility to determine what requirements must be met by a cloud service and to ensure the providers they choose can meet those requirements.

Acknowledgments

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the authors and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

Among the sources of quoted material in this document are United States government publications. Further information about copyright is available from the U.S. Copyright Office at https://www.copyright.gov.

ISC2 has created the CCSP course with the inclusion and incorporation of material from the following copyrighted works.

- Amazon Web Services (2019, August 13). Letter from Stephen Schmidt, Vice President, Chief Information Security Officer, Amazon Web Services, to Sen. Ron Wyden. August 26, 2019 re: Capital One's Amazon Web Services S3 buckets
- https://www.wyden.senate.gov/imo/media/doc/081319%20Amazon%20Letter%20to%20Sen%20Wyden%20RE%20Consumer%20Data.pdf
- Cloud Security Alliance (CSA). (2011). Trusted Cloud Initiative. White paper. © 2011 Cloud Security Alliance. All rights reserved. https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI_Whitepaper.pdf
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). (2014). ISO/IEC Standard 17789: 2014 Information technology—Cloud computing—Reference architecture. ISO/IEC 2014 © All Rights Reserved. https://www.iso.org/standard/60545.html

Notes

Notes

Notes

Notes

Official Textbook

The Certified Secure Software Lifecycle Professional (CSSLP) training provides a comprehensive review of information system security concepts and industry best practices covering the sex domains of the CSSLP Common Body of Knowledge (CBK):

Cloud Concepts, Architecture and Design
Cloud Data Security
Cloud Platform & Infrastructure Security
Cloud Application Security
Cloud Security Operations
Legal, Risk and Compliance

ISO/IEC 17024
Personnel Certification
#0668