Domain 1: Cloud Computing Concepts & Architectures

This domain provides the conceptual framework for the rest of the Cloud Security Alliance (CSA) Certificate of Cloud Security Knowledge (CCSK) Study Guide. It describes and defines cloud computing, sets out baseline terminology, and details the overall controls, deployment, and architectural models used in the rest of the document.

Cloud computing offers agility, resiliency, security, and economic benefits, but these are only realized with proper understanding and adoption of cloud models. Simply rehosting applications to a CSP without changes ("lift-and-shift") often fails to deliver the expected benefits and can increase costs. Effective cloud computing relies on understanding and utilizing cloud-native capabilities and services.

This domain provides the foundation for this guide, offering a common language and understanding of cloud computing for Cloud Service Customers (CSC[1]). It highlights the differences between cloud and traditional computing and guides security professionals and stakeholders in adopting cloud-native approaches for better security.

The Cloud Security Alliance aims to harmonize existing models, particularly NIST SP 800-145, ISO/IEC 22123-1:2023, and ISO/IEC 22123-2:2023, focusing on key security considerations for cloud professionals.

Learning Objectives

In this domain, you will learn to:

- Define cloud computing.
- Identify cloud computing models.
- Recognize reference and architecture models in cloud computing.
- Understand cloud security scope, responsibilities, and models.

[1] The acronym CSC is used interchangeably to mean any cloud service customer, cloud service consumer, or cloud service client.

1.1 Defining Cloud Computing

Cloud computing manages shared resources through abstraction, enabling rapid orchestration, provisioning, scaling, and decommissioning. It provides an on-demand utility model with benefits like collaboration, agility, elasticity, availability, resiliency, and cost reduction.

The following are definitions of cloud computing according to the U.S. National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC):

NIST SP 800-145 defines cloud computing as: *"[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."*[2]

ISO/IEC 22123-1:2023 defines cloud computing as: *"[A] paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning*[3] *and administration on-demand."*[4]

Both quotes lead to the same idea: The cloud pools resources like processors, memory, and storage using virtualization. The CSC requests needed resources, uses them over the network, and releases them back into the pool when finished.

1.1.1 Abstraction & Orchestration

Cloud environments rely on abstraction and orchestration to manage resources. For example, abstraction involves creating virtual machines (VM) from physical servers, while orchestration automates and coordinates the provisioning of these VMs and their networking to CSCs.

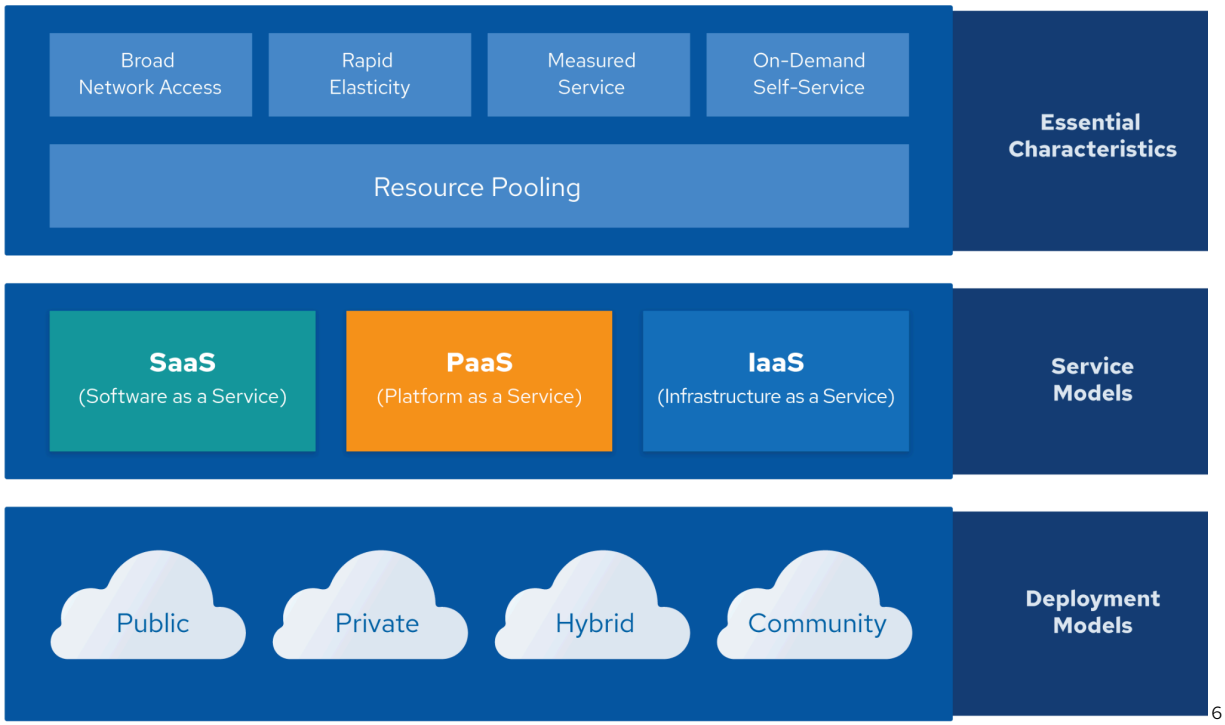
Clouds are multi-tenant, with multiple CSCs sharing resource pools while being segregated and isolated for confidentiality and integrity. Segregation and isolation ensure that CSCs cannot see or modify each other's assets. CSPs ensure fair resource use and availability by measuring and constraining overuse.

[2] NIST. (2011) SP 800-145: The NIST Definition of Cloud Computing
[3] Self-service provisioning refers to the provisioning of resources provided to cloud services performed by CSCs through automated means. Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.
[4] ISO/IEC. (2023) 22123-1:2023: Information Technology - Cloud Computing - Part 1: Vocabulary.

1.2 Cloud Computing Models

CSA uses the NIST SP 800-145 model for cloud computing as it is the standard for defining cloud computing.[5] CSA also endorses the more in-depth ISO/IEC models 22123-1:2023 and 22123-2:2023, which also serve as a reference model. Throughout this domain, we reference both.

NIST describes cloud computing based on five essential characteristics, three cloud service models, and four cloud deployment models. We summarize them below.



[6]

Figure 1: Overview of Cloud Computing Models Based on NIST and ISO/IEC Standards

1.2.1 Essential Characteristics

The NIST model describes the cloud by five essential characteristics, which set cloud computing apart from traditional hosting services or virtualization. Understanding these characteristics is critical for leveraging the full potential of cloud computing and for the strategic planning of cloud adoption.

Following are the five essential characteristics described by NIST.

[5] CSA has chosen to align with the NIST 800-145 definition of cloud computing to bring consensus around a common language and focus on use cases, rather than on semantics. This study guide is intended to be broadly applicable to organizations globally. While NIST is a U.S. government organization, the selection of this reference model should not be interpreted as excluding other points of view or geographies.
[6] Depiction of the NIST Model of Cloud Computing

- **Resource Pooling:** Cloud computing pools various physical and virtual resources to serve multiple CSCs through a *multi-tenant* model. These resources, like storage, processors, memory, and network bandwidth are dynamically assigned and reassigned according to demand.

- **Broad Network Access:** Services are available over the network and accessed through web browsers or specialized applications while using heterogeneous thin client platforms (e.g., mobile phones, laptops, IoT devices, and tablets).

- **Rapid Elasticity:** Resources are rapidly and elastically provisioned, in some cases automatically. To the CSC, the provisioned capabilities often appear unlimited and can be purchased in any quantity at any time.

- **Measured Service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, bandwidth, active user accounts). Resource usage can be measured, monitored, controlled, and reported, providing transparency for both the CSP and the CSCs of the utilized service. This enables billing based on usage, which promotes cost efficiency and accountability (pay-as-you-go model).

- **On-Demand Self-Service**: A CSC can unilaterally request cloud resources on demand for automatic provisioning by the CSP and computing capabilities, such as computing time and network storage, as needed without requiring human interaction with each CSP.

ISO/IEC 22123-2:2023 lists six key characteristics, the first five being identical to the NIST characteristics listed above. The only addition is multi-tenancy, which is distinct from resource pooling.

1.2.2 Cloud Service Models

NIST defines three service models describing the different foundational categories of cloud services. These categories are flexible; some cloud services span these tiers, while others don't fit a single model. It's a descriptive tool, not a rigid framework.

Cloud technologies evolve rapidly, making some reference models obsolete. This section provides fundamentals to help security professionals understand emerging models. We recommend ISO/IEC 22123-3 and NIST 500-292 for in-depth reference architectures. Both approaches are valid, but since the NIST model is more concise and broadly used, it is the definition predominantly used in CSA research.

Cloud computing can be viewed as a stack: Software as a Service (SaaS) on Platform as a Service (PaaS) on Infrastructure as a Service (IaaS). While this is not representative of all real-world deployments, it is a useful model.

1.2.2.1 Infrastructure as a Service

IaaS offers access to a resource pool of fundamental computing infrastructure, such as network, or storage. In IaaS the CSC is responsible for managing the underlying virtual infrastructure, such as VMs,

networking, storage, and running applications. IaaS relies on physical infrastructure, abstracted and orchestrated into resource pools. Abstraction through virtualization frees resources from physical constraints, while orchestration uses application program interfaces (APIs) to tie these resources together and deliver them to CSCs.

APIs facilitate orchestration and are often accessible through web-based interfaces, forming the cloud management plane. This management plane allows CSCs to manage resources such as VMs and networks. Security-wise, it differs from on-premises protection, as management interfaces are network-accessible, posing risks if compromised.

Here is an extremely simplified architectural example of a compute IaaS platform:

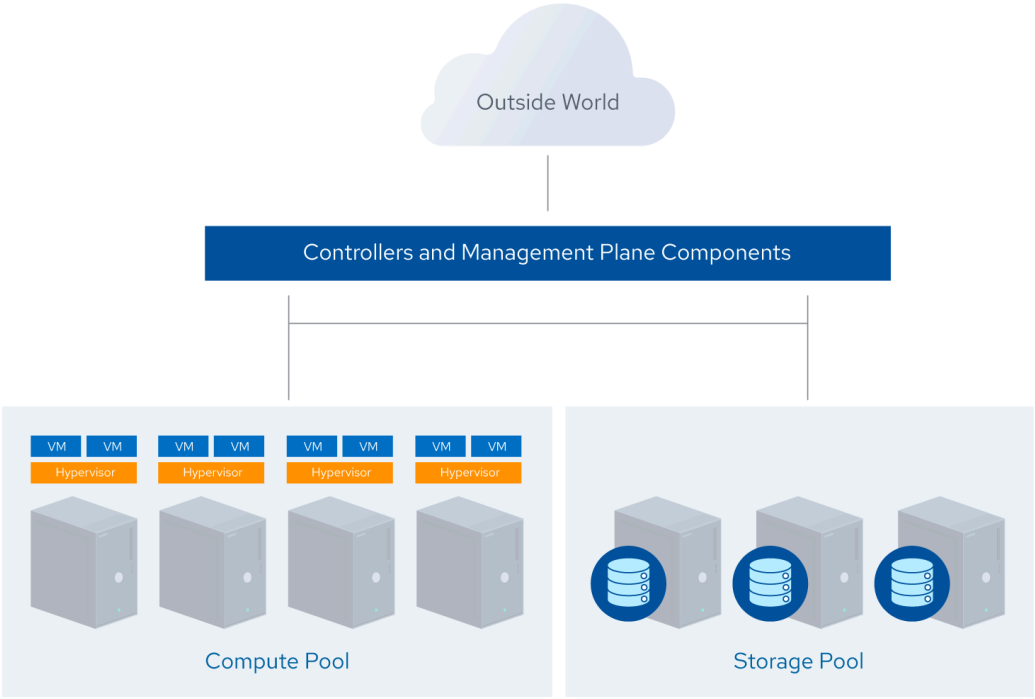


Figure 2: Simplified Architecture of an IaaS Compute Platform

This example showcases an IaaS compute platform with physical servers running hypervisors and orchestration software. The cloud controller allocates resources, creates virtual instances, configures networking and storage, and brokers connectivity information for CSCs to access the instances.

1.2.2.2 Platform as a Service

PaaS abstracts and provides platforms, such as application platforms (e.g., a place to develop and run code), databases, file storage, and collaborative environments. Other examples include application processing environments for machine learning, big data processing, or API access to SaaS functions. The key differentiator with IaaS is that, with PaaS, the CSC does not manage the underlying servers.

Often, PaaS is built on IaaS, where integration, persistence, and middleware layers are orchestrated and accessed through APIs. For example, Database as a Service (DBaaS) lets CSCs manage databases via API or web console without handling the underlying infrastructure.

In PaaS, CSCs see only the platform, not the infrastructure. The database service scales with use, removing the need for CSCs to manage and patch servers, networking, or the underlying operating system.

The following is a simplified architecture diagram that shows a PaaS running on top of an IaaS architecture.

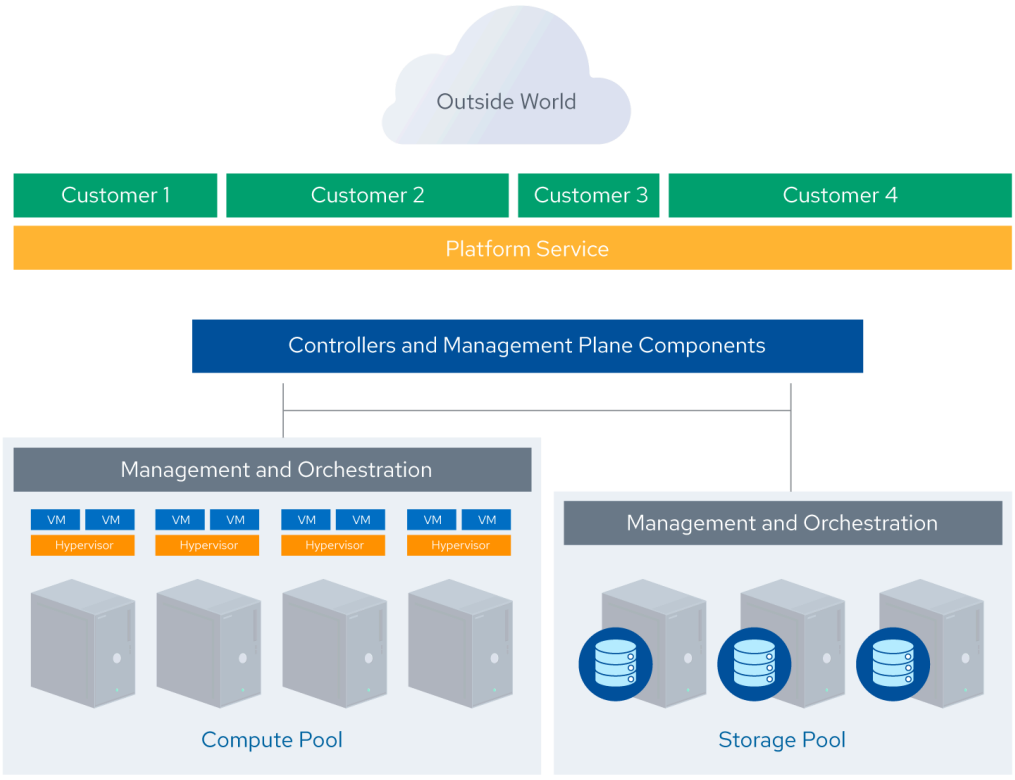


Figure 3: Simplified Architecture of a PaaS Built on IaaS

PaaS can be a custom-built, stand-alone architecture, not necessarily on IaaS. CSCs manage the platform, not the underlying infrastructure. An example is a custom AI and ML service for AI development tools, MLOps, and AI lifecycle management.

1.2.2.3 Software as a Service

SaaS services are complete applications, encompassing all the architectural complexities typical of any large software platform. It is managed by the CSP. SaaS CSPs often build on top of IaaS and PaaS due to the increased agility, resilience, and economic benefits. CSCs access it using a web browser, mobile application, APIs, or lightweight client applications. In this model, the CSC only worries about the application's configuration, not the underlying resources.

SaaS services typically include an application/logic layer, data storage, APIs, and presentation layers supporting web browsers, mobile apps, and Internet API access. The architecture diagram is generalized from a real SaaS platform.

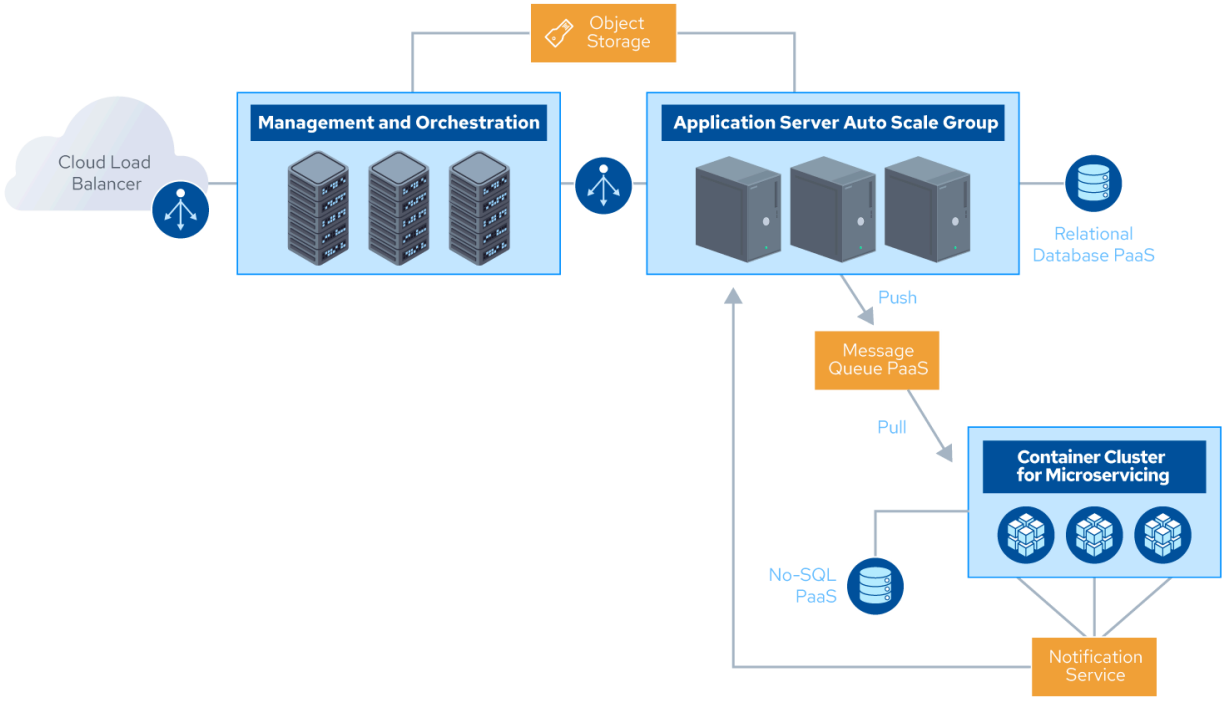


Figure 4: Simplified Architecture of a SaaS Platform Built on PaaS and IaaS

1.2.3 Cloud Deployment Models

NIST and ISO/IEC use the same four cloud deployment models; these define how the technologies are deployed, consumed, and applied across the entire range of service models.

- **Public Cloud**: The cloud infrastructure is made available to the general public or a large industry group and is owned by a CSP.
- **Private Cloud**: The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party and may be located on-premises or off-premises.
- **Community Cloud:** The cloud infrastructure is shared by several organizations and supports a specific community with shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the CSC(s) or a third party and may be located on-premises or off-premises.
- **Hybrid Cloud:** The cloud infrastructure is a composition of two or more clouds (i.e., private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

While these are the official definitions, the common use of these terms has shifted. In particular, private cloud is now being used more often to just denote a private datacenter, independent of the level of automation in provisioning that it offers, and hybrid cloud mostly refers to where such data centers are combined with one or more public cloud solutions.

1.2.4 CSA Enterprise Architecture Model

The CSA Enterprise Architecture (EA) is both a methodology and a set of tools. It is a framework, that is, a comprehensive approach for the architecture of a secure cloud infrastructure. It can be used to assess opportunities for improvement, create roadmaps for technology adoption, identify reusable security patterns, and assess various CSPs and security technology vendors against a common set of capabilities.

To create the CSA EA, CSA Research has leveraged four industry standard architecture models across the following four domains:

- **Business Operation Support Services (BOSS)** – Sherwood Applied Business Security Architecture (SABSA)
- **Information Technology Operation Services (ITOS)** – Information Technology Infrastructure Library (ITIL)
- **Technology Solution Services (TSS)**, including Infrastructure (InfraSrv), Information (InfoSrv), application (AS), and Presentation (PS) Services – The Open Group Application Framework (TOGAF)
- **Security and Risk Management (SRM)** – OpenGroup Security Forum (formerly known as the Jericho Forum)

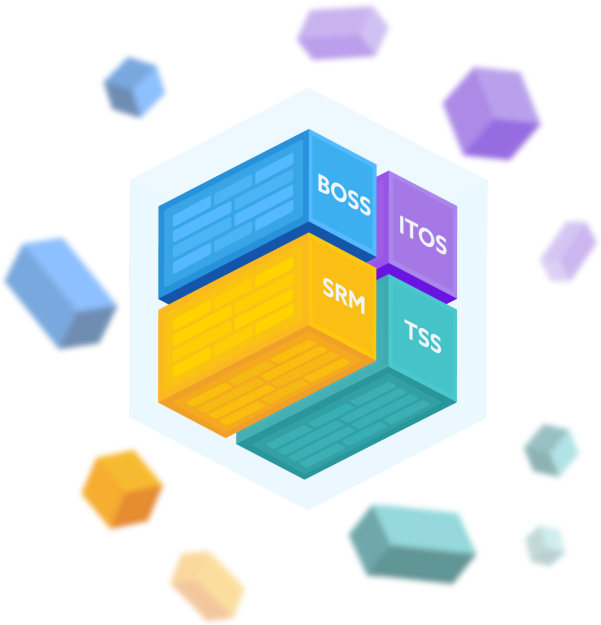


Figure 5: Building Blocks of the CSA Enterprise Architecture

CSA combines the best architecture paradigms into a comprehensive approach to cloud security while merging business drivers. The CSA EA supports the value proposition of cloud services within an enterprise business model.

The CSA EA was adopted by NIST SP 500-292, solidifying the importance of the CSA approach.

1.3 Cloud Security Scope, Responsibilities, & Models

In cloud computing, security is a joint effort known as "shared responsibility." CSPs handle the security "of the cloud," covering infrastructure, hardware, and network. CSCs manage security "in the cloud," and are responsible for their deployments. Responsibilities vary with service models.

1.3.1 Shared Security Responsibility Model

The delineation of responsibilities differs for IaaS, PaaS, and SaaS, and often between different CSPs. CSCS must understand where the demarcation lies to ensure that they are appropriately protecting their own cloud tenants, applications, data, etc., and to provide baselines for holding CSPs accountable.

At a high level, security responsibility maps to the degree of control a given actor has over the architecture stack.

- **SaaS:** The CSP handles most security, while the CSC manages authorization and entitlements. Example: The CSP manages perimeter security and logging, and the CSC manages user permissions.
- **PaaS:** The CSP secures the platform, and the CSC secures its implementations. Example: The CSP handles patching and core configuration, and the CSC manages database security features and authentication.
- **IaaS:** The CSP handles foundational security, and the CSC manages all built infrastructure. Example: The CSP monitors the perimeter, and the CSC defines virtual network security.

Roles become complex with cloud brokers and intermediaries. Knowing where a CSP's responsibility ends and its CSC's begins is crucial. CSCs must understand their obligations, especially in configuration and management, to ensure security policies align with data sensitivity.

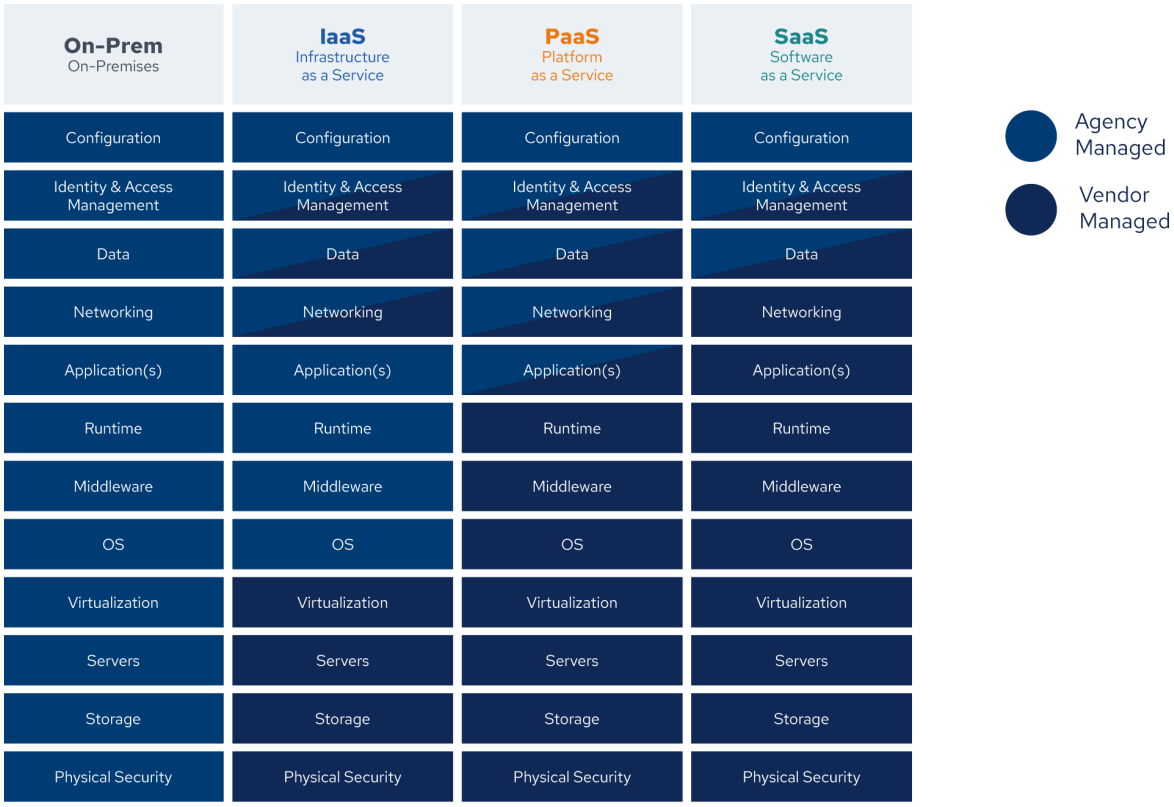


Figure 6: Shared Security Responsibility Model[7]

Effective cloud security requires understanding the division of responsibility in cloud environments. Knowing who is responsible is crucial, allowing CSCs to fill control gaps or consider alternative CSPs. Direct security control is highest for IaaS and lower for SaaS.

To ensure a clear allocation of security responsibilities in the cloud, we recommend the following:

- CSPs should document security controls and CSC features, and design and implement them properly. Often such a document is called a "shared security responsibility matrix."
- CSCs should create a roles-and-responsibilities matrix to track security responsibilities and ensure compliance alignment.

CSA provides tools to help meet these requirements:

- The Consensus Assessments Initiative Questionnaire (CAIQ) is a standard template for CSPs to document their security and compliance controls.
- The Cloud Controls Matrix (CCM), discussed in more detail in Domain 2, lists cloud security controls and maps them to multiple security and compliance standards. The CCM can also be used to document security responsibilities.

Both documents provide a comprehensive starting template and can be especially useful for ensuring compliance requirements are met.

[7]CISA. (2021) Cloud Security Technical Reference Architecture.