Domain1 Cloud Computing Concepts & Architectures

Defining Cloud Computing

Cloud Service Customers (CSC)
Cloud Security Alliance (CSA)

- **NIST SP 800-145** :
  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."
- **ISO/IEC 22123 :**
  Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.
- **abstraction**: involves creating virtual machines (VM) from physical servers.
- **orchestration** automates and coordinates the provisioning of these VMs and their networking to CSCs.
- Segregation and isolation: CSCs cannot see or modify each other's assets.

Cloud Computing models:

- CSA uses the NIST SP800-145 model + endorses **ISO/IEC 22123 as reference.

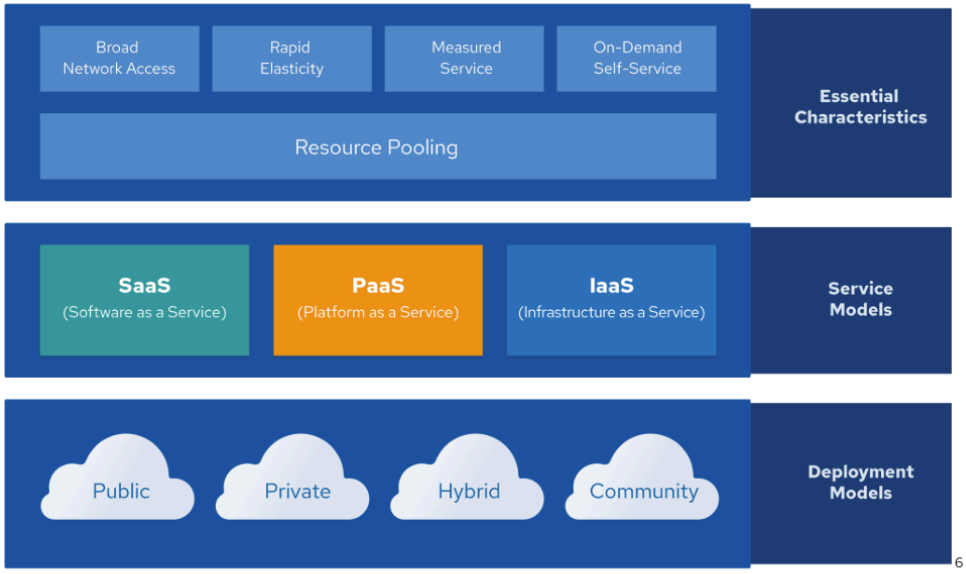

Figure 1: Overview of Cloud Computing Models Based on NIST and ISO/IEC Standards

five essential characteristics described by **NIST**:

- **Resource Pooling**: resources, like storage, processors, memory, and network bandwidth are dynamically assigned and reassigned according to demand.
- **Broad Network Access**.
- **Rapid Elasticity**: the provisioned capabilities often appear unlimited and can be purchased in any quantity at any time.
- **Measured Service:** a metering capability for billing based on usage and resource optimization.
- **On-Demand Self-Service**

SIX essential characteristics described by ****ISO**= (5 of NIST + **multi-tenancy** characteristic)

- NIST model is more concise and broadly used.

Infrastructure as a Service

- the **CSC is responsible** for managing the underlying virtual infrastructure, such as VMs, networking, storage, and running applications.
- APIs facilitate orchestration + accessible through web-based interfaces = **the cloud management plane.** (*posing risks if compromised as security*)

Platform as a Service

- The key differentiator with IaaS is that, with PaaS, the CSC does not manage the underlying servers.
- Provides platforms, such as application platforms.
- Often, PaaS is built on IaaS + CSCs see only the platform, not the infrastructure.

Software as a Service

- managed by the CSP.
- often build on top of IaaS and PaaS due to the increased agility, resilience, and economic benefits.
- CSC only worries about the application's configuration, not the underlying resources.

Cloud deployment models

- **Public Cloud:** made available to the general public
- **Private Cloud:** solely for a single organization
- **Community Cloud:** by several organizations
- **Hybrid Cloud:** The cloud infrastructure is a composition of two or more clouds (i.e., private, community, or public)

CSA Enterprise Architecture Model

- It is a **framework**, approach for the architecture of **a secure cloud infrastructure** (4 best architecture paradigms):
  - Business Operation Support Services (**BOSS**)
  - Information Technology Operation Services (**ITOS**)
  - Technology Solution Services (**TSS**)
  - Security and Risk Management (**SRM**)

- **Shared security responsibility matrix** : a document made by CSP containing security controls and CSC features . It can be created based on the **Cloud Controls Matrix (CCM)** and the **CAIQ** docs (*useful for ensuring compliance requirements are met.*)