Study Questions for NIST SP 500-292: Cloud Computing Reference Architecture

Conceptual Reference Model & Major Actors

List and define the five major actors in the NIST Cloud Computing Reference Architecture.

- **Cloud Consumer:** A person or organization that maintains a business relationship with, and uses services from, Cloud Providers.
- **Cloud Provider (CSP):** A person, organization, or entity responsible for making a service available to Cloud Consumers.
- **Cloud Auditor:** A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.
- **Cloud Broker:** An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.
- **Cloud Carrier:** An intermediary that provides connectivity and transport of cloud services between Cloud Consumers and Cloud Providers.

Describe the primary interactions between a Cloud Consumer, Cloud Provider, and Cloud Broker.

A Cloud Consumer may request cloud services directly from a Cloud Provider. Alternatively, a Cloud Consumer might engage a Cloud Broker to manage their cloud service usage. The Cloud Broker can act as an intermediary, potentially combining services from multiple Cloud Providers or adding value to a Cloud Provider's service before delivering it to the Consumer. The Consumer interacts directly with the Broker, who in turn interacts with the Provider(s).

What is the role of a Cloud Auditor, and why is this role particularly important for government agencies?

A Cloud Auditor conducts independent examinations of a Cloud Provider's service controls, security, privacy, and performance. They verify conformance to standards and policies. This role is particularly important for government agencies because it provides a mechanism for independent verification of security controls and compliance with regulations, which is often a requirement for handling sensitive government data and ensuring public trust.

Explain the three categories of services a Cloud Broker can offer. Provide an example for one category.

- **Service Intermediation:** The broker enhances or adds value to a given service. *Example: A broker providing enhanced security monitoring on top of a standard IaaS offering.*
- **Service Aggregation:** The broker combines and integrates multiple services (potentially from different providers) into a new, composite service.
- **Service Arbitrage:** Similar to aggregation, but the services are not fixed. The broker dynamically chooses services from multiple providers, often to optimize for cost or performance.

Scope of Control

How does the scope of control for a Cloud Consumer differ across IaaS, PaaS, and SaaS models regarding the Operating System and Applications?

- **IaaS:** The Cloud Consumer has control over the Operating System (guest OS), deployed applications, storage, and potentially some networking components. The provider manages the underlying infrastructure (host OS, hypervisor, physical hardware).
- **PaaS:** The Cloud Consumer has control over their deployed applications and possibly application hosting environment configurations. They do not manage the OS, middleware (beyond configuration), or underlying infrastructure.
- **SaaS:** The Cloud Consumer has the least control, typically limited to user-specific application configuration settings. The provider manages the application, OS, middleware, and all underlying infrastructure.

Architectural Components

What are the three layers in the Service Orchestration stack described in NIST SP 500-292? Briefly describe the function of each.

- **Service Layer:** This is the top layer where Cloud Providers define interfaces for Cloud Consumers to access computing services (SaaS, PaaS, IaaS).
- **Resource Abstraction and Control Layer:** This middle layer contains system components (e.g., hypervisors, virtual machines, virtual storage) that Cloud Providers use to abstract physical resources and manage access to them. It enables resource pooling, dynamic allocation, and measured service.
- **Physical Resource Layer:** This is the lowest layer, which includes all physical computing resources like hardware (CPUs, memory, networks, storage) and facility resources (HVAC, power).

Name the three main categories of Cloud Service Management and provide two examples of functions within each category.

- **Business Support:**
  - Customer Management (e.g., account setup, user profiles)
  - Accounting and Billing (e.g., managing billing information, processing payments)
- **Provisioning and Configuration:**
  - Rapid Provisioning (e.g., automatically deploying cloud systems)
  - Metering (e.g., measuring resource usage for billing)
- **Portability and Interoperability:**
  - Data Portability (e.g., copying data objects into or out of a cloud)
  - System Portability (e.g., migrating a VM image from one provider to another)

Explain "Data Portability" and "Service Interoperability" as aspects of Cloud Service Management. Why are they important for Cloud Consumers?

- **Data Portability:** The ability for Cloud Consumers to easily move their data into or out of a cloud service, or between different cloud services, without significant re-creation or modification. This often involves using standard formats or tools for bulk data transfer.

- **Service Interoperability:** The ability for Cloud Consumers to use their data and services across multiple cloud providers, potentially with a unified management interface. This allows different cloud services to communicate and work together.
- **Importance:** These are important for consumers to avoid vendor lock-in, enabling them to switch providers, integrate services from different providers, or bring data back on-premises if needed, with minimal disruption and cost.

From a security perspective, why is it important to consider both the service model (IaaS, PaaS, SaaS) and the deployment model (Public, Private, etc.)?

- **Service Model:** Different service models expose different attack surfaces and involve varying levels of consumer control, thus impacting security responsibilities. For example, in IaaS, the consumer is responsible for securing the guest OS and applications, while in SaaS, the provider handles most of this. Security concerns for SaaS might focus more on web application security and data protection, whereas IaaS might involve hypervisor security and network segmentation.
- **Deployment Model:** The deployment model affects the level of trust and the types of threats. A public cloud has a broader, more diverse set of tenants and potentially higher exposure, making workload isolation and boundary controls critical. A private cloud, dedicated to one organization, might have different trust boundaries and security priorities, though it still requires robust security. Hybrid clouds introduce complexity in securing data and applications across different environments.

What does the "Shared Security Responsibility" model imply for a Cloud Consumer using an IaaS service?

For an IaaS service, the "Shared Security Responsibility" model implies:

- **Cloud Provider's Responsibility ("Security OF the Cloud"):** Securing the physical data center, the network infrastructure, the virtualization layer (hypervisor), and the host operating systems.
- **Cloud Consumer's Responsibility ("Security IN the Cloud"):** Securing the guest operating systems they deploy (patching, hardening), the applications they install, their data (including encryption and access control), user access management (IAM), and network configurations within their virtual environment (e.g., firewalls, security groups).

Cloud Taxonomy

What is the purpose of the Cloud Taxonomy presented in NIST SP 500-292?

The Cloud Taxonomy provides a structured, hierarchical classification of cloud computing concepts, roles, activities, and components using a controlled vocabulary. Its purpose is to:

- Provide a clear and unambiguous way to describe and categorize elements of cloud computing.
- Facilitate common understanding and communication among different stakeholders (e.g., government agencies, providers, consumers).
- Support the analysis and comparison of cloud services and architectures.

The NIST Cloud Taxonomy is structured in four levels. What are these levels?

- **Level 1: Role** (e.g., Cloud Consumer, Cloud Provider)
- **Level 2: Activity** (e.g., Service Deployment, Service Orchestration)

- **Level 3: Component** (e.g., Private Cloud, Service Layer)
- **Level 4: Sub-component** (e.g., Electronic Transfer, Physical Transfer under the "Cloud Distribution" component of the "Cloud Carrier" activity)