Domain 4: Organization Management

Introduction

Most organizations use multiple SaaS CSPs and have various deployments within IaaS/PaaS CSPs. Many cloud footprints develop organically, including mergers, acquisitions, and consolidations, making cloud sprawl common.

Organization Management involves managing an entire cloud footprint, including securing and validating CSP deployments. These top-level security concerns include structuring deployments for optimal scope and security control. Despite differences in CSP technologies, there is enough feature parity for consistent management.

Learning Objectives

In this domain, you will learn to:

- Manage organization-level security within a CSP.
- Leverage organization hierarchy for managing critical aspects of cloud deployments.
- Recognize security considerations for hybrid/multi-cloud deployments.
- Identify different cloud organization hierarchy models.

4.1 Organization Hierarchy Models

There are various models of organization hierarchy utilized in cloud environments, each having their own complexities of managing cloud resources across different CSPs. As CSCs expand their use of cloud technologies, understanding the structural differences and terminology used by major CSPs like AWS, Azure, and Google Cloud is crucial. This section aims to clarify these concepts and present a standardized approach to discussing and implementing organizational structures in the cloud.

4.1.1 Definitions

Different CSPs use different words for similar organizational structures. Here are the terms that are used in this study guide:

- An "**organization**" denotes the highest level of structure within a CSP cloud provider.

- A "**group**" represents a collection of deployments.
- A "**deployment**" refers to an isolated environment within a CSP cloud provider.

Below is a brief overview of the different terminology used by the major CSPs.

Cloud Service Provider	Organization	Group	Deployment
AWS	Organization	Organization Units	Accounts
GCP	Organizations	Folders	Projects
Microsoft Azure	Tenant	Management Group	Subscription

Table 2: Cloud Service Provider Terminology Comparison

Utilizing multiple deployments is a strategic approach to reducing the impact of adverse events or breaches, adhering to service limits imposed by CSPs, and facilitating the logical separation of different technology stacks. This approach highlights the importance of using a structured and hierarchical system to organize cloud resources. This method improves security and makes it easier to manage resources in different cloud environments.

The figure below illustrates the hierarchical structure for cloud resource management across different CSPs, helping to visualize the similarities and differences:

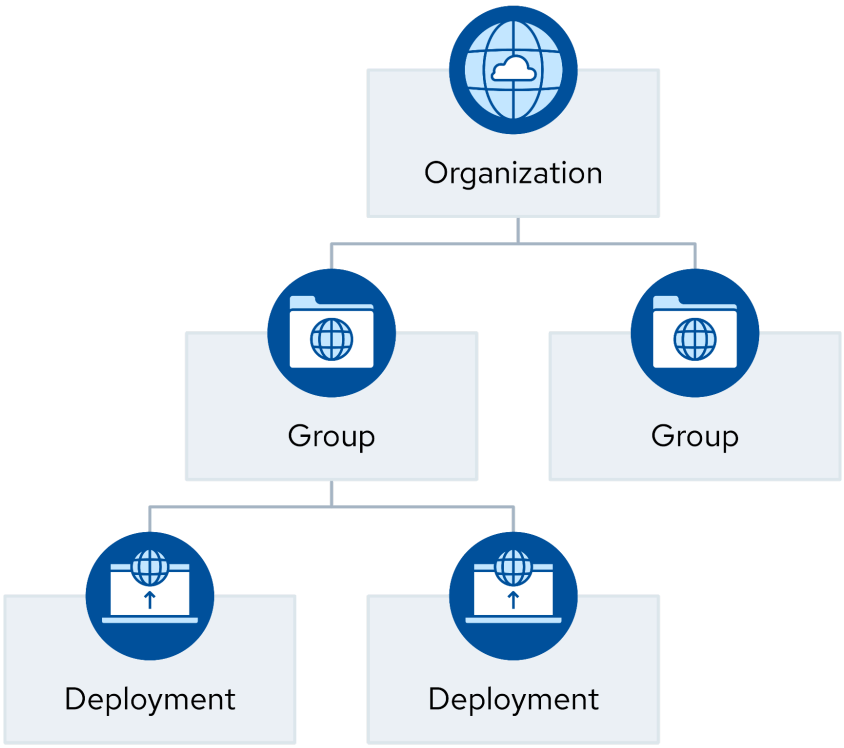

Figure 12: Hierarchical Structure for Cloud Resource Management

4.1.2 Organization Capabilities Within a Cloud Service Provider

Segmentation and segregation of organization units and different application environments are important for resilience and reducing the 'blast radius' (potential extent) of a security breach.

There are four main capabilities that all major CSPs offer that enable CSCs to significantly enhance security across their cloud environments:

- Groups allow CSCs to structure their deployments into an isolation hierarchy.
- Policies are sets of security rules that can apply to a group or a deployment. These typically enable and disable features, often down to specific API calls or even individual parameters.
- Identity and Access Management (IAM) centralization and/or federation supports centralized management of an organization's users and their entitlements.
- Each CSP supports their own set of shared security services. These vary greatly, but support for central logging is nearly always available.

In order to maintain consistency over many deployments in an organization, a CSP landing zone or account factory can be used. This is a pre-configured template that sets up and manages cloud accounts with standardized configurations, security policies, and governance controls. By automating the creation and setup of new accounts, it ensures that each deployment adheres to the CSC's best practices and compliance requirements from the start. This approach simplifies management, enhances security, and ensures uniformity across multiple accounts and projects within the cloud infrastructure.

4.1.3 Building a Hierarchy Within a Provider

CSCs typically adopt one of three models to define their hierarchy, each with its own advantages and operational implications. No single model is universally superior, and some CSCs may combine elements from different models to best reflect their operational realities:

- **Business Unit and Application-Based:** This model structures the cloud hierarchy with business units at the top, followed by applications within these units, and then environments (e.g., production vs. development). It aligns well with business-unit-focused IAM hierarchies but may be less efficient for policy management unless cloud features closely align with business units and applications.

- **Environment-Based:** Prioritizes environments (eg., development, production, testing) at the top, followed by business units or applications. It benefits policy management by establishing baseline security and operational policies for different environments but may not align well with IAM hierarchies or billing and cost management needs.

- **Geography-Based:** This model starts with geographic regions (e.g., EMEA, NA, specific countries) at the top, followed by business units or environments. It benefits global CSCs with diverse security and regulatory requirements specific to each region.

4.2 Managing Organization-Level Security Within a Provider

Organization-level security refers to controls set at the organization or group level, outside individual deployments. The goal of cloud security is to maintain acceptable risk without introducing friction that reduces or eliminates the benefits of cloud computing. It Is important to maintain control of the cloud footprint without impeding business objectives. CSPs offer a range of capabilities to support governance and security outside traditional security domains like network or application security. This starts with a well-defined tenant structure, which can be extended with additional controls.

4.2.1 Identity Provider & User/Group/Role Mappings

As mentioned above, the highest level of aggregation of deployments is the Organization. At this level, identity management determines who can access and manage deployments. These capabilities are defined by an identity provider and a set of user/group role mappings. This is potentially separate from IAM inside the deployment[24].

At this highest level, there are two important factors to consider:

- Minimize root access to limit high-level alterations or privilege escalations.
- Restrict who can create deployments, but enable teams to easily create new deployments for their environments (e.g., development, sandbox, production) that match the policies in the team's hierarchy. This is where the landing zones and account factories can accelerate those teams.

Within the organization hierarchy that is enabled by these CSPs, technical policies can define security parameters across deployments. This external positioning ensures that even administrators with complete control over a specific deployment cannot modify or delete the policies.

CSP policies can be categorized into three levels based on their scope:

1. **Organization-wide policies** are defined by the customer and apply to every deployment within the CSC. Typically, this category includes a limited set of policies due to the challenges in managing exceptions on such a broad scale.

2. **Group-level policies** that cover all deployments within a specific group. This level is most commonly used for policy application, with the ability for policies at this level to accumulate and reinforce one another, especially when applied to sub-groups. The combined set of policies is enforced by the CSP, with policies that deny actions almost always taking precedence over policies at lower levels.

3. **Deployment-level policies** are tailored for individual deployments, allowing for precise security adjustments. While applying policies at the group level is generally considered better

[24] Additional material is provided in Domain 5: *Identity and Access Management*.

management practice, certain scenarios necessitate deployment-level policies, particularly for deployments with specific and granular security requirements.

Policies can be used in various scenarios, including:

- Enabling and disabling specific services, such as prohibiting the use of an unapproved platform service for deployment.
- Blocking particular API calls to prevent unauthorized or harmful operations.
- Disabling regions to comply with geographic regulatory requirements and maintaining data residency and sovereignty requirements.
- Defining conditions like permitting specific API calls only from authorized network sources/IP addresses. However, this requires both CSP and service-level support, representing one of the more inconsistent capabilities across providers.
- Implementing IAM practices to secure organization-level access and operational tools, including preventing a deployment administrator from restricting access to critical visibility and control accounts (e.g., in the event administrator credentials are compromised).

4.2.2 Common Organization Shared Services

While individual deployments are isolated from one another, CSCs typically strive to have a degree of policy and risk management consistency across them. Until this point, we have discussed policies as a tool for that. In this section, we review a number of shared services that can be used across deployments to support those policies.

Arguably the single most important shared service for cloud security and governance is consolidated IAM across deployments. This is discussed in more detail throughout this study guide.

Centralized logging and security telemetry collect security feeds to a single destination, simplifying security monitoring, threat detection, analysis, and compliance. This is useful for sending telemetry to a Security Information and Event Management (SIEM) platform or security data lake[25].

CSP Threat Detection services continuously monitor for malicious activities and unauthorized behaviors, safeguarding deployments by identifying threats in real-time for prompt response[26].

Centralized cost management is often implemented through tagging policies, which allow for allocation of costs to specific applications, or business functions.

Finally, a relevant organizational tool is account factories. These are facilitated by Infrastructure as Code (IaC)[27].

[25] Additional material is provided in Domain 6: *Security Monitoring*.
[26] Additional material is provided in Domain 6: *Security Monitoring* and Domain 11: *Incident Response*.
[27] Additional material is provided in Domain 7: *Infrastructure & Networking*.

4.3 Considerations for Hybrid & Multi-Cloud Deployments

In today's diverse IT landscape, CSCs often rely on both hybrid and multi-cloud environments to meet their operational needs. Hybrid cloud deployments connect on-premises data centers with public cloud services, enhancing flexibility and scalability while presenting unique security challenges. Multi-cloud strategies, on the other hand, involve using multiple CSPs to avoid vendor lock-in and optimize performance – but they also increase complexity in security management. This section explores the key considerations for securing hybrid and multi-cloud environments, focusing on effective organization management, IAM, network security, and the strategic use of security tools.

4.3.1 Organization Management for Hybrid Cloud Security

A hybrid cloud integrates an existing data center or facility with a public cloud provider using a virtual private network (VPN) or dedicated network link. Domain 7 provides a detailed exploration of the networking aspects involved in this integration.

To achieve strong hybrid cloud security, CSCs should ensure robust security measures in both cloud and data center environments. If there are weaknesses in either area, they are isolated and compartmentalized to prevent vulnerabilities from affecting the other environment.

Key areas to focus on for hybrid cloud security include:

1. **Identity and Access Management (IAM):** A compromised identity provider can impact both the cloud and data center environments. Therefore, maintaining a strong IAM system is crucial.
2. **Network Security:** Weak network security can increase the attack's blast radius across both environments. Stringent network security measures should be implemented to protect against such threats.

It is important not to normalize security controls between hybrid cloud environments, as cloud technologies and data centers have significant differences. Using a single set of controls for both can create security gaps and failures. Instead, appropriate tools and strategies should be tailored to each environment.

Hybrid cloud sprawl, resulting from connecting multiple data centers to numerous cloud deployments through various VPNs or dedicated links and multiple identity providers, can increase security challenges. To mitigate this, connection sprawl should be minimized. Mature CSCs often consolidate connectivity into a central “bastion network” to govern all traffic flows between deployments, simplifying management and enhancing security.

4.3.2 Organization Management for Multi-Cloud Security

The concept of multi-cloud is often used to describe the usage of multiple IaaS/PaaS CSPs. Attempting this strategy before achieving maturity with one creates significant security challenges. Each CSP is fundamentally different, requiring a deep understanding of its unique characteristics. Supporting multiple CSPs with shared security services is very difficult.

CSCs should not move to a second IaaS CSP until they have an effective security program for their primary CSP. However, mergers, acquisitions, or business requirements often result in multi-cloud environments. This challenge can be managed with adequate expertise, effective management strategies, and key security-shared services designed for multi-cloud.

There are three strategies for organizing for multi-cloud:

- **Single provider:** The organization uses one CSP for IaaS deployments. If an additional CSP is added due to merger or acquisition, that deployment is migrated to the primary CSP.
- **Primary/secondary:** All new deployments go to a primary CSP, representing the CSC's main cloud footprint. Additional CSPs are used for limited or isolated deployments, approved only if the primary CSP cannot meet specific needs or due to merger or acquisition. Secondary CSPs are tightly locked down and use minimal services to reduce security and operational complexity.
- **Full multi-cloud support:** The CSC equally supports two or more major CSPs.

Ideally, a CSC starts with a single CSP and then adds compartmentalized islands as additional CSPs as needed, until mature enough to support multiple CSPs. However, many CSCs are forced into multi-cloud situations before maturity due to practical realities, internal politics, and business relationships.

For CSCs adopting containers[28], one common misperception of multi-cloud is that a cloud-agnostic container strategy will support fully portable workloads that allow the CSC to pick any CSP at any point in time, possibly for dynamic cost management. In reality, there are significant obstacles to achieving a cloud-agnostic implementation. These are as much operational as security challenges:

- Containers create workload portability but not management infrastructure portability. There is still considerable overhead in building out the runtime and orchestration environments for the containers.
- Shared services are typically less portable unless they are also fully stateless and containerized. Databases, message queues, notification buses, and other services that underlie modern applications are typically better served by a CSP service on dedicated, non-portable resources,
- A CSC may lose economic, security, and operational benefits provided by PaaS services from the CSP.

[28] Additional material is provided in Domain 8: *Cloud Workload Security*.

4.3.2.1 Tooling & Staffing for IaaS/PaaS Multi-Cloud

Many CSCs transition to the cloud without increasing staffing, forcing existing staff to develop cloud skills while supporting traditional infrastructure.

Each CSP demands specific domain knowledge. The more services consumed, the wider the knowledge needed. CSCs should have at least one subject matter expert for each significant cloud platform. A primary/secondary strategy can reduce the need for dedicated experts.

Smaller organizations often shift the burden of skilled staffing to Managed Service Providers (MSPs), but this does not shift accountability for security and governance. The MSP's vision, strategy, and capabilities should align with the desired future state of the CSC.

4.3.3 Organization Management for SaaS Hybrid & Multi-Cloud

CSCs leverage various SaaS CSPs to enhance operations and innovation. Unlike IaaS, where consolidation and CSC security responsibilities are higher, SaaS presents challenges due to diverse offerings and diverging security maturity.

Effective SaaS security management starts with diligent portfolio management. SaaS CSPs should be evaluated for security and compliance measures before authorization to handle specific data types. This process should be documented in a central registry. New SaaS CSPs within an already serviced category should require strong business justification.

SaaS solutions often require integrations with other applications, facilitating data flow. Governance over these integrations is required to maintain security and control over data movement.

Three types of tools can help management of multiple SaaS CSPs within a security program:

1. **Federated Identity Brokers**: With pre-built integrations for major CSPs, and a unified dashboard for user access to different services, federated identity brokers significantly streamline the CSC and lifecycle administration of user access and permissions for all cloud models, SaaS in particular.

2. **Cloud Access and Security Brokers (CASB)**: CASBs can be very useful for managing a CSC's SaaS portfolio, offering access control and monitoring capabilities, and enforcing which SaaS CSCs are utilized, by which users, and from where.

3. **API Gateways**: Interactions between SaaS applications and other applications generally work over APIs. API gateways can bring visibility, control, and policy enforcement over these interactions.