Domain 4 Organization Management

- "**Organization**"denotes the highest level of structure within a CSP cloud provider.
- "**Group**"represents a collection of deployments.
- "**Deployment**"refers to an isolated environment within a CSP cloud provider.

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

- Segmentation and segregation of organization units = **resilience and reducing the 'blast radius'**
- **CSP landing zone** or account factory = 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 = c**ompliance requirements from the start.**

Building a Hierarchy Within a Provider

- **Business Unit and Application-Based:** aligns well with business-unit-focused IAM hierarchies and **less efficient for policy management**.
- **Environment-Based:** Prioritizes environments (eg., development, production, testing) at the top, followed by business , 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.
- administrators with complete control over a specific deployment cannot modify or delete the policies. cz hierarchy enabled by CSP.
- CSP policies can be categorized into **three levels** based on their scope:
  - **Organization-wide policies**
  - **Group-level policies**
  - **Deployment-level policies**
- The single **most important shared service for cloud security** and governance is **consolidated IAM across deployments**
- Centralized logging and security telemetry
- CSP Threat Detection services
- Centralized cost management
- **Hybrid cloud sprawl**: resulting from connecting multiple data centers to numerous cloud deployments through various VPNs or dedicated links > ==increase security challenges .
- CSCs should not move to a second IaaS CSP until they have an effective security program for their primary CSP.

- 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.**
- 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.
  - CSCs should have **at least one subject matter expert for each significant cloud platform.**
  - Smaller organizations often shift the burden of skilled staffing to Managed Service Providers (MSPs)

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.