Certified Cloud Security Professional

(CCSP)

Notes by Al Nafi

Domain 3

Cloud Platform & Infrastructure Security

Author:

Osama Anwer Qazi

Chapter 6: Responsibilities in the Cloud

1- Foundations of Managed Services

Managed services in the cloud refer to **outsourced IT functions** provided by **Cloud Service Providers (CSPs)** to help businesses manage their infrastructure, applications, and security. These services reduce operational overhead, improve security, and ensure compliance.

Key Characteristics of Managed Services:

- **Outsourced IT Management:** Cloud providers handle infrastructure, security, and operations.
- **Automation & Monitoring:** Continuous monitoring of cloud resources using AI/ML.
- **Scalability & Availability:** Ensures high availability, backup, and disaster recovery.
- **Cost Efficiency:** Pay-as-you-go pricing models minimize upfront investments.

Common Cloud Managed Services:

Service Category	Examples
Compute Management	AWS EC2 Auto Scaling, Azure Virtual Machine Scale Sets
Database Services	AWS RDS, Azure SQL Database, Google Cloud Spanner
Security & Compliance	AWS Security Hub, Azure Security Center, Google Security Command Center
Networking & Load Balancing	AWS ELB, Azure Traffic Manager, Google Cloud Load Balancer

Backup & Disaster Recovery	AWS Backup, Azure Site Recovery, Google Cloud Storage Backup

Best Practices for Managed Services:

✅ Clearly define Service Level Agreements (SLAs).
✅ Continuously monitor service performance and security settings.
✅ Enforce identity and access controls for managed services.

2- Business Requirements

Cloud adoption must align with business requirements to ensure security, compliance, and operational efficiency.

Business Requirements: The Cloud Provider Perspective

Cloud providers must meet specific business needs, including:

1. **Security & Compliance:** Ensure alignment with ISO 27001, GDPR, HIPAA, and SOC 2.
2. **Service Uptime & Availability:** Meet SLA guarantees (e.g., 99.99% uptime).
3. **Scalability & Performance:** Support dynamic resource allocation for businesses.
4. **Data Residency & Sovereignty:** Provide options for regional data storage.
5. **Integration & Interoperability:** Ensure compatibility with third-party applications.

Best Practices:

✅ Select a CSP that meets your security and compliance needs.
✅ Regularly review SLAs, service performance, and costs.
✅ Define data residency policies before choosing cloud regions.

3- Shared Responsibilities by Service Type

Cloud security responsibilities vary depending on the service model: IaaS, PaaS, or SaaS.

IaaS Responsibilities:

Responsibility	Cloud Provider	Customer
Infrastructure Security	Manages physical data centers, networking, and hypervisors.	Configures firewalls, storage, and IAM.
Virtual Machines & Storage	Provides VM templates and scalable storage.	Manages OS patches, encryption, and backups.
Network Security	Provides basic network security options.	Configures **VPNs, firewalls, and access controls.**

✅ **Best Practice:** Implement network segmentation, encryption, and secure access policies.

PaaS Responsibilities:

Responsibility	Cloud Provider	Customer
Platform & Middleware Security	Manages OS, runtime, and middleware.	Secures **applications and APIs.**
Data Storage & Encryption	Provides encrypted storage options.	Configures **IAM and data protection policies.**

✅ **Best Practice:** Use **secure coding practices and API security controls.**

SaaS Responsibilities:

Responsibility	Cloud Provider	Customer
Application & Infrastructure Security	Manages entire application stack.	Configures **user access and authentication (MFA, SSO).**
Data Protection & Compliance	Ensures regulatory compliance.	Defines **data retention policies and encryption.**

✅ **Best Practice:** Implement **Zero Trust security, MFA, and data loss prevention (DLP).**

4- Shared Administration of OS, Middleware, or Applications

In cloud environments, administration responsibilities are split between CSPs and customers.

Operating System Baseline Configuration and Management

- **CSP Responsibility:**
    - Provides secure OS images and automated patching.
    - Manages underlying host infrastructure and hypervisors.
- **Customer Responsibility:**
    - Hardens OS configurations (disable unnecessary services, enforce access control).
    - Regularly updates and patches OS vulnerabilities.
    - Implements endpoint protection and monitoring tools.

✅ **Best Practice:** Use OS baseline configurations (CIS Benchmarks, NIST guidelines).

5- Shared Responsibilities: Data Access

Cloud consumers and CSPs share responsibility for **data access control.**

Customer Directly Administers Access

- Customers manage IAM policies, role-based access control (RBAC), and MFA.
- Ensures least privilege access to sensitive data.

✅ **Best Practice:** Implement **IAM best practices and conduct periodic access reviews.**

Provider Administers Access on Behalf of the Customer

- CSPs manage admin-level access to cloud-hosted applications.
- Customers must ensure CSPs follow security best practices (SOC 2, ISO 27001).

✅ **Best Practice:** Define clear access control policies and monitor CSP activities.

Third-Party (CASB) Administers Access on Behalf of the Customer

- Cloud Access Security Brokers (CASBs) enforce security policies for SaaS applications.
- CASBs provide DLP, shadow IT detection, and threat intelligence.

✅ **Best Practice:** Deploy CASBs to monitor and enforce SaaS security policies.

6- Lack of Physical Access

Since cloud environments are remotely managed, customers lack physical access to cloud infrastructure.

Audits

- Customers rely on third-party audit reports (SOC 2, ISO 27001, FedRAMP).

- CSPs conduct regular security audits and provide compliance certifications.

✅ **Best Practice:** Review CSP audit logs and request compliance reports.

Shared Policy

- CSPs provide security frameworks and compliance tools.
- Customers must enforce cloud security policies (IAM, encryption, monitoring).

✅ **Best Practice:** Align security policies with cloud provider recommendations.

Shared Monitoring & Testing

- CSPs provide logging tools (AWS CloudTrail, Azure Monitor, Google Cloud Logging).
- Customers must analyze logs and detect threats.

✅ **Best Practice:** Use SIEM solutions to correlate security events and automate incident response.

Conclusion

1. Foundations of Managed Services ensure automated security, monitoring, and compliance.
2. Business Requirements must align with SLA guarantees, compliance mandates, and scalability needs.
3. Shared Responsibilities by Service Model define security roles for IaaS, PaaS, and SaaS.
4. Shared OS & Middleware Administration requires strong baseline configurations and patching policies.
5. Data Access Responsibilities vary across customer, provider, and third-party-managed access.
6. Lack of Physical Access requires reliance on audits, shared policies, and monitoring tools.

By understanding shared responsibilities and security best practices, organizations can enhance cloud governance, reduce risks, and ensure regulatory compliance.

Further Reading & References:

- **AWS Shared Responsibility Model:** https://aws.amazon.com/compliance/shared-responsibility-model/
- **Microsoft Azure Security Center:** https://learn.microsoft.com/en-us/security/
- **Google Cloud IAM Best Practices:** https://cloud.google.com/iam/docs/best-practices

These resources provide deep insights into cloud security responsibilities and compliance strategies.