**MODULE 5**

1. Planning and Assessment

**Risk Assessment**:

Identify potential security threats and vulnerabilities specific to your cloud environment.

Conduct regular assessments to understand the security posture.

**Compliance Requirements**:

Determine relevant regulations (e.g., GDPR, HIPAA, PCI-DSS) that apply to your data and operations.

Develop policies and procedures to meet these requirements.

**Access Control and Identity Management**

**Identity and Access Management (IAM)**:

Implement IAM solutions to manage user identities and permissions.

Use Role-Based Access Control (RBAC) to limit access based on job functions.

**Multi-Factor Authentication (MFA)**:

Require MFA for all users accessing cloud resources to enhance security.

**Regular Access Reviews**:

Conduct periodic audits of user access rights and adjust them as necessary.

**Data Protection**

**Data Encryption**:

Encrypt data at rest and in transit using strong encryption algorithms (e.g., AES).

Utilize cloud provider encryption tools (e.g., AWS KMS, Azure Key Vault).

**Data Loss Prevention (DLP)**:

Implement DLP solutions to monitor and protect sensitive data from unauthorized access and sharing.

**Backup and Recovery**:

Regularly back up critical data and establish a disaster recovery plan to restore data in case of loss.

**Network Security**

**Firewalls and Security Groups**:

Use cloud-native firewalls and security groups to control inbound and outbound traffic.

Configure rules to restrict access to only trusted IP addresses.

**Virtual Private Network (VPN)**:

Utilize VPNs to create secure connections for remote access to cloud resources.

**Intrusion Detection and Prevention Systems (IDPS)**:

Deploy IDPS to monitor network traffic for suspicious activity and respond accordingly.

**Monitoring and Logging**

* **Continuous Monitoring**:

Implement monitoring tools (e.g., AWS CloudTrail, Azure Monitor) to track user activity and resource usage.

Set up alerts for unusual behavior or policy violations.

* **Logging**:

Enable logging for all critical activities and regularly review logs for signs of security incidents.

Retain logs for an appropriate period to support audits and investigations.

2. Portability in cloud computing refers to the ability to move applications, data, and workloads between different cloud environments or between on-premises systems and the cloud without significant constraints or rework.

3. Reliability refers to the ability of a cloud service to consistently perform its intended function without failure. It measures the likelihood that a system will operate correctly over a specified period.

High availability (HA) is the design and implementation of systems that ensure a high level of operational performance and uptime, typically quantified as a percentage of uptime.

4**.** **Mobility Cloud Computing** refers to the integration of cloud computing with mobile technologies, enabling access to cloud-based services and applications through mobile devices.

5. AWS is a comprehensive cloud services platform provided by Amazon, offering a wide range of services for computing, storage, databases, machine learning, analytics, and more.

Microsoft Azure is a cloud computing platform that offers a wide range of services, including computing, analytics, storage, and networking, tailored for businesses and developers.

Google Cloud Platform offers a suite of cloud computing services, emphasizing data analytics, machine learning, and container orchestration.