Domain 5 Identity and Access Management (IAM) Exam Prep Summary

1. Introduction to IAM in Cloud Computing

Identity and Access Management (IAM) ensures that only **authorized users, devices, and systems** can access cloud resources. In cloud environments, IAM is the **new security perimeter**, replacing traditional network boundaries.

Key Differences Between Cloud & On-Prem IAM

1. **Shared Responsibility Model:** CSPs manage infrastructure IAM, while customers control access to their data.
2. **Multiple IAM Systems:** Cloud providers use different IAM models, adding complexity.
3. **Internet-Exposed Interfaces:** Cloud IAM APIs and consoles require strict security.

🔷 *Most cloud breaches occur due to IAM misconfigurations!*

---

2. Fundamental IAM Concepts

IAM consists of key security principles that define **identity**, **authentication**, **authorization**, and **entitlements**.

Concept	Definition
Access Control	Restricts access based on CRUD (**C**reate, **R**ead, **U**pdate, **D**elete) permissions.
Identity	Attributes that uniquely identify a user, system, or device.
Authentication	**Verifies identity** using credentials (passwords, MFA, tokens).
Authorization	Determines **access rights** based on **roles**, **policies**, or **attributes**.
Multifactor Authentication (MFA)	Requires multiple authentication factors (e.g., password + OTP, biometrics).
Entitlement	Maps identities to authorizations via an entitlement matrix.
RBAC (Role-Based Access Control)	Assigns access based on predefined roles (e.g., Admin, Developer).
ABAC (Attribute-Based Access Control)	Grants access based on dynamic attributes (e.g., location, device).
PBAC (Policy-Based Access Control)	Uses policy documents for flexible access control.

3. Identity Federation & Standards

🔷 What is Federation?

Federation allows users to **authenticate once** and access multiple systems using **Single Sign-On (SSO)**.

🔷 **Key Components:**

- **Identity Provider (IdP):** Authenticates users and issues identity assertions.
- **Relying Party (RP):** A cloud service that **grants access based on IdP verification.**
- **Assertion:** A statement from IdP confirming user identity and attributes.

Common Federation Standards

Protocol	Use Case
SAML	XML-based, used for enterprise authentication.
OAuth 2.0	API authorization (e.g., Google Login).
OpenID Connect (OIDC)	Adds authentication to OAuth for web services.

💡 *SAML is best for enterprises, OAuth for API authorization, and OIDC for cloud services!*

4. IAM Architectures in Cloud

Organizations must decide how to integrate IAM with cloud providers.

Federation Architectures:

1️⃣ **Hub & Spoke Model:** A **central identity broker** handles authentication across cloud providers. ✔ Best for large enterprises needing centralized IAM.

2️⃣ **Free-form Model:** Internal directory services connect directly to CSPs.
❌ Riskier, as it exposes directories to the internet.

💡 ***Hub & Spoke ensures better security governance!***

5. Authentication & Authorization Best Practices

🔷 Authentication Mechanisms

✓ **Passwords (weakest, should be avoided)**
✓ **MFA (OTP, hardware tokens, biometrics)**
✓ **Passwordless authentication (FIDO keys, certificates)**
❌ Avoid passwordless authentication for privileged accounts!_

🔷 Access Control Models

Model	Description
RBAC	Assigns roles (e.g., Admin, User) for predefined access.
ABAC	Uses attributes (device, location, risk score) to grant access.
PBAC	Implements policy-driven, machine-readable access rules.

💡 _**ABAC & PBAC** provide better flexibility than RBAC!_

---

6. Privileged Access Management (PAM & PIM)

✓ **Privileged Identity Management (PIM):** Manages elevated roles and temporary admin access. ✓ **Privileged Access Management (PAM):** Controls access methods and session monitoring.

🔷 **PAM Best Practices:**
✅ Enforce **MFA** for all privileged accounts.
✅ Use **session recording & auditing** to monitor activity.
✅ **Rotate credentials automatically** to prevent leaks.

💡 *PAM prevents unauthorized privilege escalation and insider threats!*

---

7. IAM Best Practices for Cloud Security

🔷 **Essential IAM Controls:**
✓ Enforce **MFA** for all cloud accounts.
✓ Use **RBAC, ABAC, or PBAC** to limit access.
✓ **Monitor IAM logs** for anomalies.
✓ **Audit IAM policies** regularly.
✓ **Use Just-In-Time (JIT) access** to reduce exposure.

💡 *IAM misconfigurations are a leading cause of cloud breaches!*

---

8. Exam Tips & Key Takeaways

🎯 **Understand IAM models** (RBAC, ABAC, PBAC).
🎯 **Know Federation Standards** (SAML, OAuth, OpenID Connect).
🎯 **Master IAM security controls** (MFA, PAM, Just-In-Time access).
🎯 **Be able to analyze IAM architectures & workflows.**

💡 *Most IAM questions test your ability to apply security principles in cloud environments!*
