

Exam Cram Notes: Identity and Access Management (IAM)

1. Overview

Identity and Access Management (IAM) involves managing the identification of users, devices, and applications and controlling their access to network resources. The goal of IAM is to ensure that only authorized users and systems can access specific resources at the right times and for the right reasons.

2. Core Components of IAM

✓ **Authentication** – Verifying the identity of users or systems.

- **Methods:** Passwords, Multi-Factor Authentication (MFA), Biometrics, Smart Cards.
 - ✓ **Authorization** – Defining what authenticated users can do, i.e., their level of access.
 - **Access Control Models:** Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC).
 - ✓ **Accounting (Auditing)** – Tracking user activity and resource access for compliance and analysis.
 - **Logs and Reports:** Access logs, event logs, audit trails.
 - ✓ **Identity Federation** – Allowing users to use a single identity across multiple systems or organizations.
 - **Protocols:** SAML (Security Assertion Markup Language), OAuth, OpenID Connect.
-

3. Authentication Methods

✓ **Single Sign-On (SSO)** – Allows users to authenticate once and gain access to multiple systems without re-entering credentials.

✓ **Multi-Factor Authentication (MFA)** – Requires multiple verification methods (something you know, something you have, something you are).

- Examples: Password + SMS code, fingerprint + PIN, hardware token + facial recognition.
 - ✓ **Biometric Authentication** – Uses physical characteristics (e.g., fingerprints, retina scans, facial recognition) for verification.
 - ✓ **Smart Cards / Tokens** – Physical devices that generate one-time codes or store credentials for secure login.

◆ MFA Best Practices:

- Use at least two independent factors (e.g., password and fingerprint).
- Require MFA for access to sensitive resources or remote access.

4. Access Control Models

✓ **Discretionary Access Control (DAC)** – The resource owner determines access rights.

- Example: File system permissions on personal devices.

✓ **Mandatory Access Control (MAC)** – Access decisions are based on predetermined policies.

- Example: Government systems with classified information.

✓ **Role-Based Access Control (RBAC)** – Access is granted based on roles within an organization.

- Example: HR staff can access payroll, but not IT systems.

✓ **Attribute-Based Access Control (ABAC)** – Access is granted based on policies that evaluate attributes (e.g., user's department, time of day).

- Example: Only users in the "Finance" department can access financial records during business hours.
-

5. Identity Federation & Single Sign-On (SSO)

✓ **Identity Federation** – Allows users to authenticate once and access systems across multiple organizations or platforms.

- Example: Logging into a third-party service using Google or Facebook credentials.

✓ **SSO Protocols:**

- **SAML (Security Assertion Markup Language)** – Used for exchanging authentication and authorization data between identity providers and service providers.
 - **OAuth** – A token-based authorization framework that allows access to resources without sharing credentials.
 - **OpenID Connect** – An identity layer built on top of OAuth to verify user identity.
-

6. Privileged Access Management (PAM)

✓ **Privileged Accounts** – Accounts with higher privileges (e.g., administrator accounts).

✓ **Least Privilege Principle** – Users and systems should be granted the least amount of access necessary for their tasks.

✓ **Just-in-Time (JIT) Access** – Grants elevated privileges only for the time needed and revokes them after use.

✓ **PAM Tools:**

- CyberArk, BeyondTrust, Thycotic, and other PAM solutions help manage, monitor, and audit privileged account access.
-

7. Identity Governance and Administration (IGA)

- ✓ **IGA Solutions** – Help ensure the proper assignment of access rights and comply with regulatory requirements.
 - ✓ **Access Certification** – Regular review of user access to ensure it is still appropriate.
 - ✓ **Separation of Duties (SoD)** – Prevents any user from having excessive power (e.g., preventing one user from approving and processing financial transactions).
 - ✓ **User Provisioning & De-provisioning** – Automating the creation and removal of user accounts.
-

8. Identity as a Service (IDaaS)




- ✓ **Cloud-Based IAM Solutions** – Provides centralized identity management without on-premises infrastructure.
 - ✓ **Key Providers:**
 - Okta, Microsoft Azure Active Directory (Azure AD), Ping Identity, OneLogin.
 - ✓ **Benefits of IDaaS:**
 - Scalable and flexible for cloud applications and services.
 - Simplifies the management of user identities across hybrid environments.
-

9. IAM Best Practices

- ✓ **Use of Strong Password Policies** – Minimum length, complexity (uppercase, lowercase, numbers, special characters), and expiration.
 - ✓ **Regular Auditing & Reporting** – Monitor user access and ensure it aligns with business needs and compliance.
 - ✓ **Granular Access Control** – Grant access based on roles, responsibilities, and tasks, rather than broad permissions.
 - ✓ **MFA for All Critical Applications** – Enforce MFA for remote access, admin accounts, and sensitive systems.
 - ✓ **Regular Reviews & Recertifications** – Periodically review and verify user access rights to ensure compliance with the least privilege principle.
-

10. Key Exam Takeaways

- ✓ **Understand Authentication Methods:**
 - The importance of SSO, MFA, and biometrics in enhancing security.
- ✓ **Familiarize with Access Control Models:**
 - DAC, MAC, RBAC, and ABAC, and when each is applicable.
- ✓ **Implement Privileged Access Management (PAM):**

- Safeguard high-privilege accounts and enforce the least privilege principle.
 **Use Identity Federation & SSO:**
- Leverage protocols like SAML, OAuth, and OpenID Connect to provide secure, seamless access.
 **Implement Identity Governance & Administration (IGA):**
- Regularly review user roles and access rights, and prevent segregation of duties violations.
 **Apply Best Practices:**
- Strong password policies, automated provisioning/de-provisioning, regular access reviews.