Identity and Access Management (IAM)

https://IdentityArchitect.dev

- **Authentication**
  - Password Management — creating, storing, and updating user passwords securely
  - Multi-factor Authentication (MFA) — requiring users to provide two or more verification factors to gain access to a resource
  - Single Sign-On (SSO) — allows users to access multiple applications or services with one set of credentials, simplifying the login process
- **Authorization**
  - Entitlements — the specific rights and privileges a user has to access and interact with resources or data within a system.
  - Role-Based Access Control (RBAC) — assigns system access based on a user's role within an organization
  - Attribute-Based Access Control (ABAC) — grants access based on user attributes (like department or job title), environment conditions, and resource characteristics
  - Policy-Based Access Control (PBAC) — grants access to resources through policies that evaluate the context of access requests against established rules
  - Policy Enforcement — ensures that access to resources is granted or denied according to predefined security policies and rules
- **Identity Management**
  - User Registration — the process where new users provide necessary information to create an account within a system or service.
  - User Provisioning — automatically creating, updating, and managing user accounts across systems and applications
  - Profile Management — allows users to update their personal information, preferences, and security settings within an account
  - Consent Management — obtaining and tracking users' permissions for data collection, processing, and sharing, in compliance with privacy regulations
- **User Store (Directory Service)**
  - User Repositories — data stores that store and manage information about users, including their credentials, roles, and access rights
  - Group Management — organizing users into categories or groups to simplify the assignment of shared access rights and resources
  - Credential Store — securely handling the creation, storage, and updating of user credentials, like passwords and digital certificates
- **Identity Federation**
  - Security Assertion Markup Language (SAML) — standard for exchanging authentication and authorization data between parties, particularly between an identity provider and a service provider
  - OAuth2 — protocol that allows applications to securely access resources on behalf of a user without sharing the user's credentials
  - OpenID Connect (OIDC) — an authentication layer on top of OAuth 2.0 that allows applications to verify the identity of users based on the authentication performed by an authorization server
  - Social Login — allows users to access applications using their existing login information from social networking services, simplifying the authentication process
- **Privileged Access Management (PAM)**
  - Secure Admin Access — implementing security measures to control and monitor administrative users' access to critical systems and data
  - Credential vaulting — securely stores and manages sensitive information like passwords and keys, restricting access only to authorized users and applications
  - Privileged session management — controls and monitors sessions for users with elevated access rights to ensure security and compliance
  - Session Launching — initiates user sessions in a controlled environment, ensuring secure and authenticated access to systems or applications without the end user having to know the underlining credentials
- **Identity Governance & Administration (IGA)**
  - Access Requests — formal requests by users seeking permission to access specific resources, data, or applications
  - Access Request approvals — process of reviewing and granting or denying a user's request for access to certain resources
  - Access Provisioning — automatically creating, updating, and managing user and system accounts and access rights across systems and applications
  - Access Reviews — periodic evaluations conducted to ensure that users have appropriate permissions for their roles and that unnecessary access rights are revoked
  - Orchestration — automated coordination and management of processing changes to identities, accounts, and access rights across multiple systems
  - Identity Lifecycle Management — processes and technologies for creating, maintaining, and deactivating user identities and access rights across joiner, mover, and leaver events
- **Audit and Compliance**
  - Activity Monitoring — tracks and analyzes user actions within systems to ensure compliance with policies and to detect potential security threats
  - Compliance reporting — generating and analyzing reports to ensure organizational practices adhere to relevant laws, regulations, and compliance frameworks
  - Risk Analysis — assesses potential vulnerabilities and threats in order to prioritize and mitigate risks, as it relates to identity and access controls