Identity and Access Management (IAM)

IAM -Definition

Identity and Access Management (IAM) is the discipline that enables the **right individuals** to access the **right resources** at the **right times** for the **right reasons**.

IAM or **IdAM** is a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources.

- a way to tell who a user is and what they are allowed to do.
- managing a given set of users' digital identities, and the privileges associated with each identity

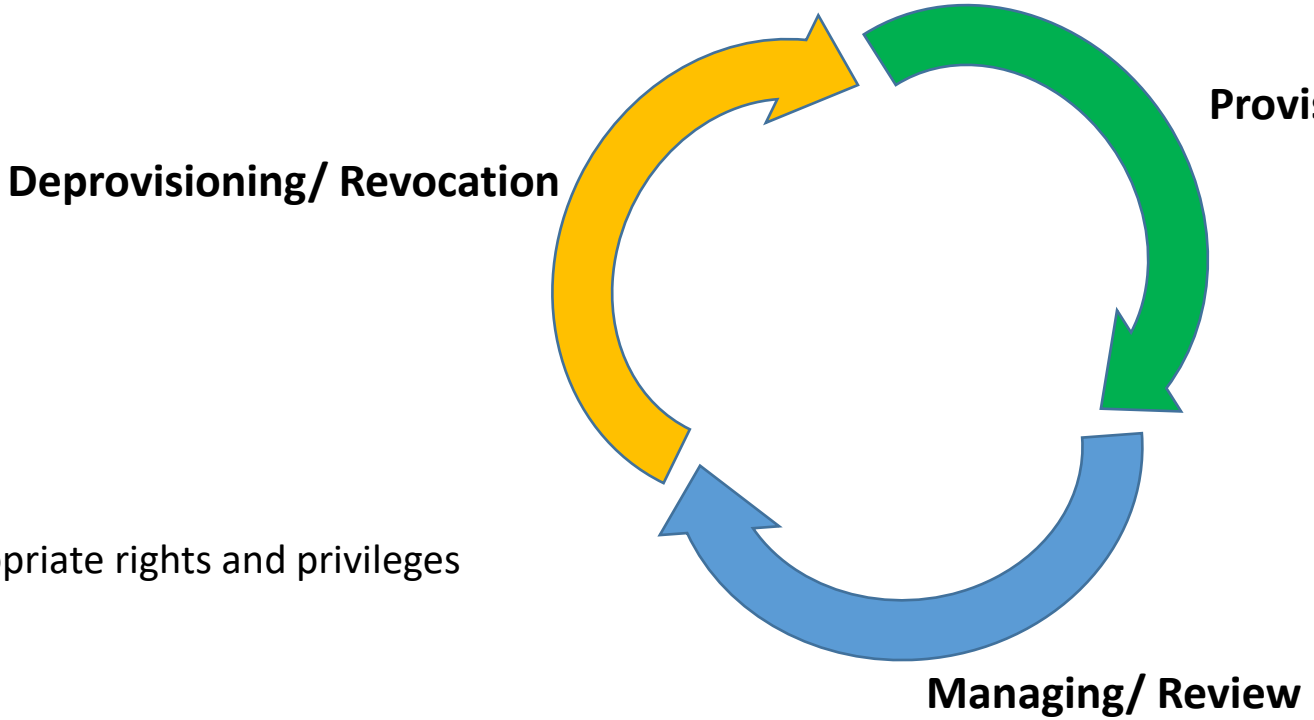
IAM

- ‘Access’ and ‘user’ are two vital IAM concepts.
  - “Access” refers to actions permitted to be done by a user (like view, create, or change a file).
    - Physical Access & Logical Access
  - “Users” could be employees, partners, suppliers, contractors, or customers. Furthermore, employees can be further segmented based on their roles.
- Other Terms related to IAM
  - Subject – The component that needs access to Objects or the Data
  - Object – The component that contains data or information

Identity Management

- **Identity management** (**ID management**) is the organizational process for **identifying**, **authenticating** and **authorizing** individuals or groups of people to have access to applications, systems or networks by associating user rights and restrictions with established identities.
- Identification- Who is the user – used on logon or database lookup
  (Identify the real entity)
- Authentication - Is this the real user? Systems needs to provide evidence!
  (Testing evidence of a user's identity)
- Authorization – Granting access to objects (if the subject is identified and authenticate properly)

Key Factors of IAM -Identity Life Cycle



Provisioning

Create new accounts & provide them the appropriate rights and privileges

Managing/Review

Check and manage accounts periodically, identify and manage excessive and creeping privileges

Deprovisioning/Revocation

Disable the account as soon as the employee leaves the company, restrict access to temporary employees based on time limit, Delete the account as per organizational policy

Key Factors of IAM -Identification

Methods used for Identification

- Username/UserID
- Account Number
- PIN
- MAC Address
- IP Address
- Email Address
- RFID

Characteristics of identity to ensure Security

Uniqueness
Non-descriptiveness
Secure issuance

Key Factors of IAM -Authentication

- Factors that affect the identification verification
  - Something you know
  - Something you have
  - Something you are

- Strong Authentication can avail by
  - Multi-Factor Authentication(MFA)

Key Factors of IAM -Authorization

- **Authorization** is a security mechanism to determine access levels or user/client privileges related to system resources including files, services, computer programs, data and application features.

- Access criteria are based on
  - Roles
  - Groups
  - Location
  - Time
  - Transaction

Features of IAM

- Password Management
  - Set Password Policies
    - Length, Complexity, Time Limit
    - Password expiry
    - Previous Login dates
    - Limit unsuccessful logins
    - Limit concurrent access
- Profile Management
  - Information related to a particular user identity or group
    - Personal information
    - Credentials
    - Rights & Privileges

Features of IAM

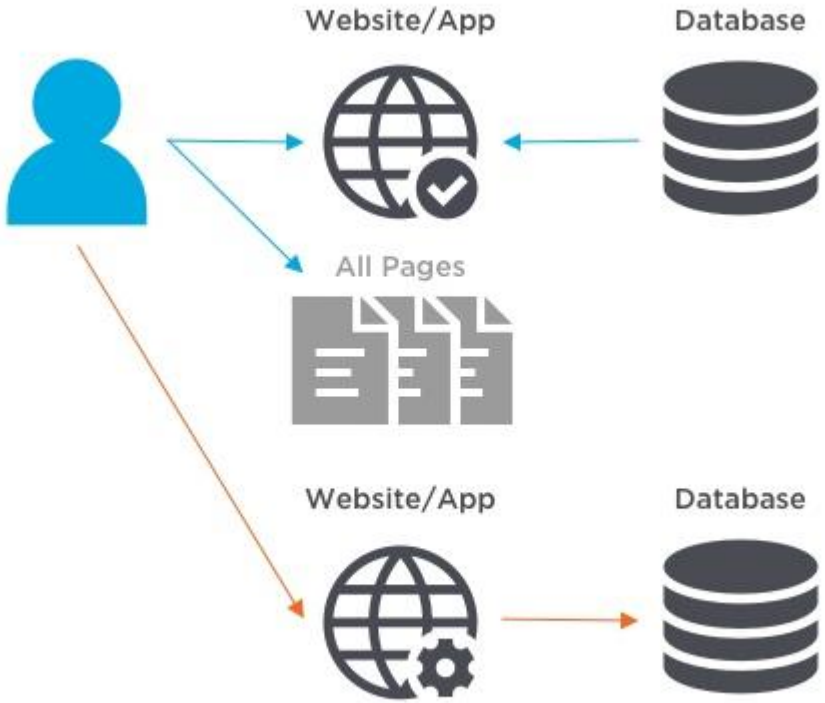
- Directory Management
  - Directory services are software programs that link directly into core databases to manage the identities and security of users on a network
  - Common Directory standards
    - **X.500** -It is a series of computer networking standards covering electronic directory services.
    - **Lightweight Directory Access Protocol(LDAP)-** It is an open and cross platform protocol used for directory services authentication.
    - **Active Directory** -Microsoft AD is by far the most common directory services system in use today.

Features of IAM

- Web Access Management (WAM)
  - It is a form of identity management that controls access to web resources, providing authentication management, policy-based authorizations, audit and reporting services (optional) and single sign-on convenience.
    - Password, digital certificate, tokens etc.
    - Act as a gateway between users and web-based resources
- Single Sign-On (SSO)
  - is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems.

Single Sign-On (SSO)

Without SSO



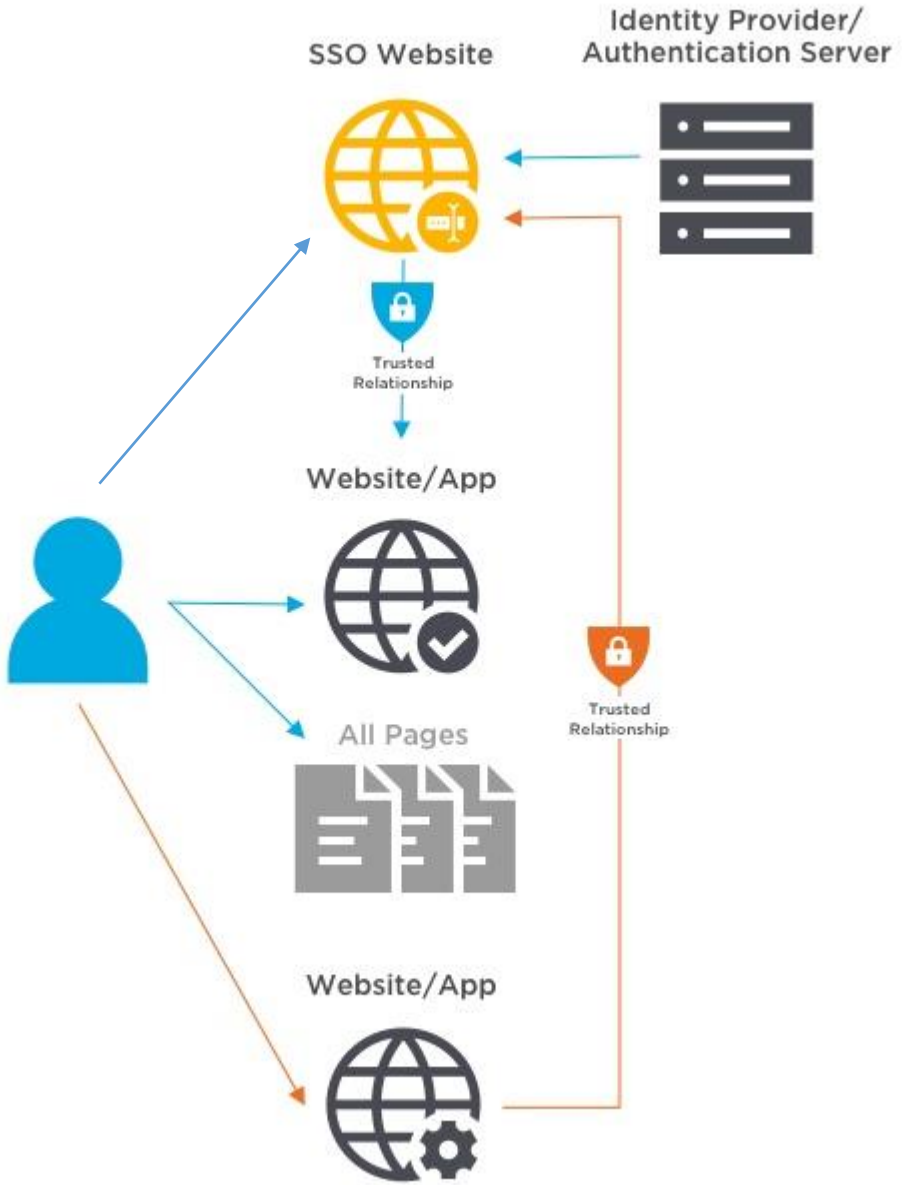


Image Courtesy- www.onelogin.com

Single Sign-On (SSO)

- Kerberos, Security Service, Domain service etc. are examples of SSO technologies

- Application of SSO
  - Google
  - AWS

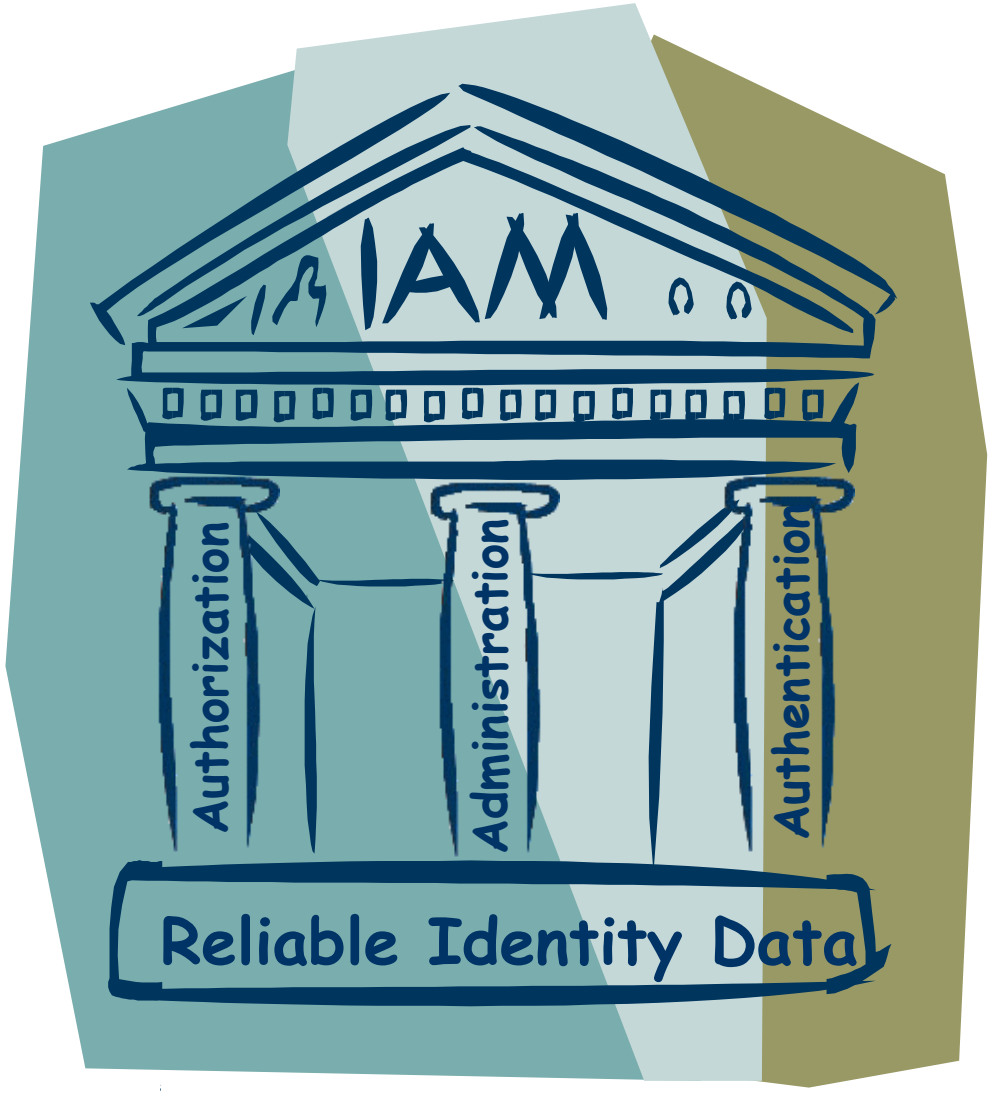
Features of IAM

Credentials Management System

- Authorities must be able to create and revoke credentials as customers and employees come and go or simply change roles, and as business processes and policies evolve.

Components of IAM

- Administration
  - User Management
  - Password Management
  - Workflow
- Access Management
  - Authentication
  - Authorization
- Identity Management
  - Account Provisioning
  - Account Deprovisioning
  - Synchronisation



IDaaS

- Identity-Management-as-a-Service (IDaaS)

- IDaaS providers :IBM, EmpowerID, Optimal IdM ,Centrify Identity Service, Ping Identity PingOne,VMware Workspace One, Centrify Identity Service, Okta identity management service, Microsoft

Cloud IAM

- IAM is a crucial aspect of cloud security

- Cloud IAM refers to the ability to manage user identities and their access to IT resources from the cloud.
  - Don’t use root accounts
  - Adopt a role-per-group model
  - Grant least-privilege

- Cloud Service - AWS, Microsoft Azure, Google Cloud ..