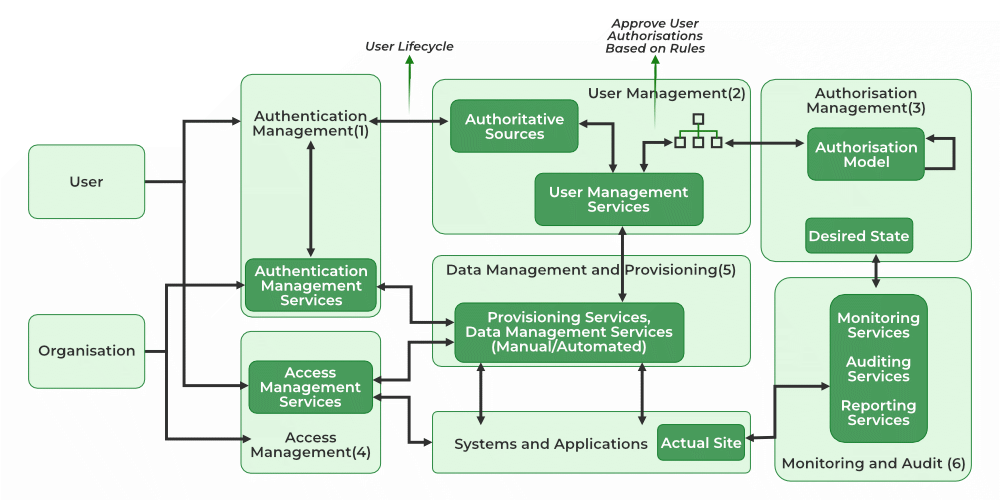
**Identity and Access Management (IAM) :**

* [**Identity and Access Management (IAM)**](https://www.geeksforgeeks.org/identity-and-access-management-iam/)**is a combination of policies and technologies that allows organizations to identify users and provide the right form of access as and when required.**
* **The services and resources you want to access can be specified in IAM. IAM doesn’t provide any replica or backup**
* **IAM can be used for many purposes such as, if one want’s to control access of individual and group access for your AWS resources.**

**IAM Components :**

* **Roles: These are defined sets of permissions that can be assigned to users. For example, an "Admin" role might have the ability to manage all resources, while a "Viewer" role can only view resources.**
* **Groups: These are collections of users who share similar permissions. Instead of assigning permissions individually, users are grouped, and permissions are assigned to the group. This simplifies management, especially in large organizations.**
* **Policies: These are documents that define permissions and rules. They dictate what actions users or groups can perform on which resources. Policies are used to grant roles to users or groups, specifying the level of access.**

**The Architecture of Identity Access Management :**



**User Management:- It consists of activities for the control and management over the identity life cycles.**

**Identity Management: Handles the creation, maintenance, and deletion of user accounts and identities.**

**Authentication Management:- It consists of activities for effectively controlling and managing the processes for determining which user is trying to access the services and whether those services are relevant to him or not.**

**Authorization Management:- It consists of activities for effectively controlling and managing the processes for determining which services are allowed to access according to the policies made by the administrator of the organization.**

**Access Management:- It is used in response to a request made by the user wanting to access the resources with the organization.**

**Data Management and Provisioning: Authorizes access to data and identities for IT resources. It Can be done through automated systems or manual methods.**

**Monitoring and Auditing : Tracks user access and activities based on defined policies. Involves monitoring usage, auditing actions, and generating reports on resource access.**

**IAM Technologies and Tools**

* **Single Sign-On (**[**SSO**](https://www.geeksforgeeks.org/introduction-of-single-sign-on-sso/)**): A choice that lets a user login and use multiple applications at once, as well as give more security to the services. Example: Its competitors include Okta and Microsoft Azure AD.**
* **Multi-Factor Authentication (**[**MFA**](https://www.geeksforgeeks.org/multifactor-authentication/)**): A second one is that you must verify your account with two or more ways to boost its security. Example: Some of the examples of Two Factor Authentication applications are Duo Security and Google Authenticator.**
* **Role-Based Access Control (**[**RBAC**](https://www.geeksforgeeks.org/role-based-access-control/)**): Secures the system based on employees’ roles, where the user will have the least privilege to access the system. Example: IBM Security Identity Manager.**
* **Privileged Access Management (**[**PAM**](https://www.geeksforgeeks.org/privileged-access-management-pam-for-linux-and-unix/)**): Performs functions associated with obtaining and maintaining high levels of accessible (“privileged”) computing resources. Example: CyberArk, BeyondTrust.**

**IAM systems offer several benefits:**

1. **Improved Security: Ensures only authorized users have access to sensitive information, reducing the risk of data breaches.**
2. **Simplified Compliance: Helps organizations comply with regulatory requirements by providing detailed audit trails and access controls.**
3. **Operational Efficiency: Automates user provisioning and deprovisioning, reducing the administrative burden on IT staff.**
4. **Enhanced User Experience: Provides seamless and secure access to resources, often with single sign-on (SSO) capabilities.**
5. **Reduced Risk: Minimizes the risk of insider threats by enforcing strict access controls and monitoring user activities.**
6. **Scalability: Easily manages access for a growing number of users and resources, making it suitable for organizations of any size.**

**IAM systems do have some drawbacks:**

1. **Complexity: Setting up and managing IAM can be complex, requiring significant expertise and resources.**
2. **Cost: Implementing and maintaining IAM systems can be expensive, especially for smaller organizations.**
3. **User Experience: If not properly configured, IAM systems can create friction for users, leading to frustration and reduced productivity.**
4. **Performance Impact: IAM can introduce latency in access requests, which might impact performance if not optimized.**
5. **Single Point of Failure: If the IAM system fails, it could potentially lock users out of all resources.**