1. Define Identity and access management (IAM)

**Answer:**

Identity and access management (IAM) is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities. With an IAM framework in place, information technology (IT) managers can control user access to critical information within their organizations. Systems used for IAM include single sign-on systems, two-factor authentication, multifactor authentication and privileged access management. These technologies also provide the ability to securely store identity and profile data as well as data governance functions to ensure that only data that is necessary and relevant is shared.

1. Identity the service components of IAM

**Answer:**

* **Authentication** - allows users to gain initial access to an application system by providing credentials. Once authenticated, a session is created, persisting until the user logs off or it's terminated.
* **Authorization -** grants access to tools and resources, defining user boundaries and jurisdictions.
* **Administration** - manages user accounts, groups, permissions, and password policies, forming the foundation for authentication and authorization.
* **Auditing and Reporting (A&R)** – track users' activities, ensuring compliance with regulations and safeguarding the system. This involves examining, recording, and reporting access logs for security purposes, adhering to regulations like CPRA, HIPAA, PCI DSS, GDPR, etc.

1. Create an IAM architecture based on your assigned capstone system

**Answer:**