Key concepts of IAM

Key concepts of IAM
IAM is a fundamental aspect of cybersecurity, ensuring that the right individuals have the appropriate access to digital resources while minimising security risks. Some key concepts relating to IAM are:

1. Digital identity: At the core of IAM lies the concept of digital identity. A digital identity represents a user within a system, application, or network and includes attributes such as username, password, and additional information that uniquely identifies an individual.
2. Authentication: Authentication is the verification of the identity of a user or system. It ensures that the person or entity trying to access a resource is who they claim to be. Common methods include password-based authentication, multi-factor authentication (MFA), and biometric authentication.
3. Authorisation: Once a user's identity is verified, authorisation determines what actions or resources that user is allowed to access. Authorisation is often based on roles, permissions, or access control lists (ACLs) that define what each user can do within a system.
4. SSO: SSO is a convenient IAM feature that allows users to log in once and gain access to multiple connected systems or applications without needing to re-enter their credentials. It enhances both user experience and security.
5. Least privilege principle: IAM follows the principle of least privilege, ensuring that users are granted the minimum level of access necessary to perform their job functions. This minimises the potential for unauthorised access.