Domain 5: Identity and Access Management (IAM)

5.1 - Control physical and logical access to assets

Information

Systems

Devices

Facilities

Applications

5.2 - Manage identification and authentication of people, devices, and services

Identity Management (IdM) implementation

Single/Multi-Factor Authentication (MFA)

Accountability

Session management

Registration, proofing, and establishment of identity

Federated Identity Management (FIM)

Credential management systems

Single Sign On (SSO)

Just-In-Time (JIT)

5.3 - Federated identity with a third-party service

On-premise

Cloud

Hybrid

5.4 - Implement and manage authorization mechanisms

Role Based Access Control (RBAC)

Rule based access control

Mandatory Access Control (MAC)

Discretionary Access Control (DAC)

Attribute Based Access Control (ABAC)

Risk based access control

5.5 - Manage the identity and access provisioning lifecycle

Account access review (e.g., user, system, service)

Provisioning and deprovisioning (e.g., on /off boarding and transfers)

Role definition (e.g., people assigned to new roles)

Privilege escalation (e.g., managed service accounts, use of sudo, minimizing its use)

5.6 - Implement authentication systems

OpenID Connect (OIDC)/Open Authorization (Oauth)

Security Assertion Markup Language (SAML)

Kerberos

Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System Plus (TACACS+)