**📘 Summary: 06 Identity and Access Management**

**1. IAM in the Operational & Organisational Models**

* Central to both daily operations and strategic controls.
* IAM includes:
  + **General Access** (for most users)
  + **Privileged Access** (for critical/administrative functions)
  + **Service Accounts** (non-human, system-based)

**2. Access Control Principles**

* **Least Privilege**: Only grant what is needed
* **Birth Rights**: Basic access (network, email, self-service)
* **Job Role Access**: Application/systems required for job
* **Privileged Access**:
  + IT admin, critical system access
  + Requires stronger control and monitoring

**3. IAM Lifecycle – JML Process**

**Joiners – Movers – Leavers**

* Integrated with HR and business processes
* Ensures:
  + Timely access provisioning/deprovisioning
  + Proper authorisation and approvals
* Supports automation and auditing

**4. IAM-Affected Capabilities**

* **Identity provisioning & deprovisioning**
* **HR, payroll, comms, business tools**
* **Access control systems**
* **Asset tracking**
* **Compliance reporting**

**5. High-Level IAM Process Steps**

1. **Provisioning Request**
2. **Identity Creation**
3. **Access Configuration**
4. **Authorisation Configuration**
5. **Business Approval**

**For PAM (Privileged Access):**

* Similar flow but includes:
  + Temporary credentials
  + Enhanced approval/authentication

**6. Key IAM/PAM Concerns**

* **IAM systems**
* **Directory services**
* **Federation & SSO**
* **MFA**
* **Access recertification**
* **Vendor/onboarding**
* **PAM system deployment & governance**

**7. IAM Standard – Key Elements**

* **Scope:** Covers all user types (staff, contractors, guests)
* **Contents:**
  + **Access prerequisites**
  + **Authentication requirements**
  + **Recertification policies**
  + **Privileged access rules**
  + **Roles and responsibilities**
  + **Compliance & exception handling**

**8. IAM/PAM Architectures**

* **IAM**: Directory + Policy + Authentication Flow
* **PAM**: Privileged vaults, session management, credential rotation

1. **Key Activities and Outputs**

| **Function** | | **Activity** | | **Output** | |
| --- | --- | --- | --- | --- | --- |
| **IAM** | | **Set up/manage systems** | | **Deployed systems** | |
| **IAM** | | **Provision/deprovision identities** | | **Defined user records** | |
| **IAM** | | **Manage user access & recertifications** | | **Audit-ready reports** | |
| **IAM** | | **Directory & federation services** | | **Documented groups/systems** | |
| **IAM** | | **System onboarding & integration** | | **Compliance-validated setup** | |
| **IAM** | | **Maintain IAM standards** | | **Documented procedures** | |
| **IAM** | | **Run MFA systems & integrations** | | **MFA system readiness** | |
| **IAM** | | **Support audits & incidents** | | **Reports/logs** | |
| **PAM** | | **Manage privileged accounts & access** | | **Secure credential distribution** | |
| **PAM** | | **Onboard and integrate systems** | | **System documentation** | |
| **PAM** | | **Maintain PAM systems** | | **Patched, up-to-date services** | |
| **PAM** | | **Respond to audits/incidents** | | **Audit outputs, forensics support** | |

**10. IAM System Types**

| **Type** | **Focus** |
| --- | --- |
| **EIAM (Enterprise IAM)** | **Internal org users, SSO, MFA, federation** |
| **CIAM (Customer IAM)** | **External customers, consent, profiles, self-service** |
| **PAM (Privileged Access Mgt)** | **Administrative & system-level control** |

**11. Service Maturity Levels**

| **Level** | **Scope** |
| --- | --- |
| **Foundation** | **Manual processes, fragmented systems** |
| **Advanced** | **Centralised IAM/PAM, SSO, governance** |
| **Optimised** | **Automated workflows, zero trust, NAC, fast JML cycles** |

**12. Framework Mapping**

**NIST CSF**

* Protect: IAM, PAM, Access Rights
* Respond: IR support
* Recover: Adjustments to services

**ISO 27001**

* A9: Access Control
* A16: Incident Management (audit logs)
* A18: Compliance (recertification)

**MITRE ATT&CK**

* IAM & PAM controls mitigate lateral movement, privilege escalation, account abuse