**Implementation of Security Controls — MFA, OAuth2, Encryption at Rest/In Transit**

**Objective:**  
Ensure end-to-end data security and user access protection through industry-standard security protocols and multi-layered defenses.

**Detailed Components:**

* **Authentication & Authorization:**
  + **OAuth 2.0** protocol for secure delegated access (mobile/web apps).
  + **JWT tokens** with short expiry and refresh mechanism.
  + **Multi-Factor Authentication (MFA):**
    - TOTP via Google Authenticator, Authy, or SMS fallback.
    - Configurable MFA enforcement per user role or device type.
* **Data Encryption:**
  + **Encryption in Transit:**
    - HTTPS with TLS 1.3 for all APIs and data transmission.
  + **Encryption at Rest:**
    - AES-256 encryption for sensitive database columns (e.g., salaries, PII).
    - Encrypted file storage (e.g., payslip PDFs, employee IDs).
* **Session & Token Management:**
  + Secure token storage using **Keychain (iOS)** and **Keystore (Android)**.
  + Auto logout on token expiry or inactivity.
* **Security Hardening:**
  + Regular vulnerability scans (e.g., OWASP ZAP).
  + Protection against XSS, CSRF, SQLi, and IDOR.