**Implementation of Security Controls (Encryption, Tokenization, Fraud Detection)**

**Objective**

Establish a robust security framework to protect financial transactions, user data, and system integrity using multi-layered security controls aligned with CBK and ISO standards.

**Implemented Controls**

| **Control Area** | **Details** | **Tools / Standards** |
| --- | --- | --- |
| **Encryption** | AES-256 for data at rest, TLS 1.3 for data in transit | OpenSSL, AWS KMS, HashiCorp Vault |
| **Tokenization** | PAN/ID masking for mobile wallet users and card-linked services | PCI DSS-compliant token vault |
| **Access Control** | Role-Based Access Control (RBAC), MFA for admins | Keycloak, Google Authenticator |
| **Fraud Detection** | Rule-based and ML-based transaction monitoring | SAS Fraud Framework, AWS Fraud Detector |
| **Audit Logging** | Immutable logs for all financial transactions and API calls | ELK Stack, Wazuh, CloudTrail |
| **Data Loss Prevention** | Field-level masking and export restrictions on PII/KYC | Symantec DLP, PostgreSQL Row Policies |
| **Threat Detection** | Real-time alerting on anomalies or suspicious API behavior | Snort, Suricata, AWS GuardDuty |

**Security KPIs**

* **Incident Response Time**: < 15 mins
* **False Positive Rate**: < 2%
* **Audit Coverage**: 100% traceable transactions
* **Uptime of Fraud Engine**: ≥ 99.95%