**Deliverable 4: Data Governance and Security Architecture**

**Description:**

This deliverable establishes a comprehensive data governance and security framework to ensure confidentiality, integrity, and availability of customer and transactional data across Safaricom's mobile money ecosystem. It also ensures compliance with internal policies, CBK guidelines, and international standards.

**Components:**

* **Data Governance Framework:**
  + Data ownership matrix (data stewards, custodians, processors)
  + Data classification policy (public, confidential, highly confidential)
  + Data lifecycle management policy (creation, usage, archiving, deletion)
  + Data lineage and traceability models (from entry to transformation and reporting)
* **Security Architecture:**
  + Multi-layered security controls (application, database, infrastructure)
  + Zero Trust Architecture enforcement with identity verification at each access point
  + Use of Hardware Security Modules (HSMs) for PIN and encryption key management
  + End-to-end encryption (E2EE) of financial transactions and KYC data
  + Data Loss Prevention (DLP) rules integrated with mail, endpoints, and storage
  + Role-Based Access Control (RBAC) integrated with LDAP/Active Directory
* **Compliance and Auditability:**
  + Automated audit trails (API and database activity logging)
  + Integration with CBK real-time reporting requirements
  + Regular internal audits and penetration testing (quarterly)
  + Data breach response and notification protocol (aligned with Kenya’s Data Protection Act)

**Techniques and Tools:**

* **Data governance tooling:** Collibra or Apache Atlas for metadata and lineage tracking
* **Security tooling:**
  + Fortinet/Check Point firewalls
  + Cloud security posture management (CSPM) for AWS/Azure
  + Splunk or QRadar for SIEM (Security Information and Event Management)
* **Key management:** AWS KMS or Thales HSMs

**Complexity and Strategic Relevance at Safaricom:**

* Must secure **financial data for 30M+ active users**, including agents and merchants.
* Involves **governance over hybrid cloud and on-prem systems** (Huawei M-Pesa Core, AWS-hosted analytics).
* Navigating **multi-jurisdictional compliance** (CBK, GDPR, and regional laws like Ethiopia’s cyber laws).
* **Real-time fraud detection integration** with external partners (e.g., NCBA, KCB, KRA).
* Establishing **data trust and visibility** across multiple Safaricom business units and partner APIs.