**Deliverable 5: Data Governance, Risk Management, and Compliance Framework**

**Description:**

This deliverable defines the policies, processes, and controls to ensure data quality, privacy, integrity, and compliance in Safaricom’s mobile money operations. It mitigates regulatory, operational, and reputational risks while enabling secure data-driven innovation.

**Components:**

* **Data Governance Policies:**
  + Data ownership and stewardship definitions
  + Data lifecycle management (creation, usage, retention, destruction)
  + Master data management for customer and transaction records
* **Risk Management Plan:**
  + Risk identification (e.g., fraud, data leakage, insider threats)
  + Risk assessment (likelihood and impact analysis)
  + Risk mitigation strategies (tokenization, redaction, access controls)
  + Business continuity planning (BCP) and disaster recovery (DR)
* **Compliance Controls:**
  + Adherence to CBK Guidelines, Kenya Data Protection Act (2019)
  + GDPR-aligned policies for handling cross-border data
  + AML/KYC enforcement, audit logging, and traceability
  + Internal audits and quarterly compliance reporting

**Techniques and Tools:**

* **Data classification matrix** and retention schedule templates
* **DLP (Data Loss Prevention)** tools (e.g., Symantec DLP, Microsoft Purview)
* **Risk Register** with continuous update cycle in Excel/SharePoint
* Integration of **SIEM systems** (e.g., Splunk, QRadar) for real-time monitoring
* Internal **compliance dashboard** for audit and policy tracking

**Complexity and Strategic Importance at Safaricom:**

* Operates in a **highly regulated financial ecosystem**, under CBK and anti-money laundering oversight.
* Must manage **petabyte-scale sensitive customer data** with multi-level access control.
* Requires coordination across **legal, risk, IT security, and product units**.
* Supports **cross-border data compliance** in regional markets (e.g., Ethiopia, Tanzania).