**Regulatory Compliance Mapping**

**Project:** Cloud Migration – Telco Core & Support Systems  
**Role:** IT Project Manager (Mid-Level)  
**Objective:** Ensure full adherence to local and international regulations during and after cloud transition.

**1. Applicable Regulations & Standards**

| **Regulation/Standard** | **Description** | **Relevance to Telco Cloud Migration** |
| --- | --- | --- |
| **GDPR** (General Data Protection Regulation) | EU regulation on personal data protection and privacy. | Applies to all customer data handling and processing—especially for Telco CRM, billing, and subscriber analytics systems. |
| **ISO/IEC 27001** | Information Security Management System (ISMS) standard. | Guides how security controls are implemented during and after cloud deployment. |
| **ISO/IEC 27017** | Cloud-specific security practices. | Ensures secure configuration and management of cloud environments. |
| **ISO/IEC 27018** | Protection of personal data in the cloud. | Relevant to customer data privacy in SaaS/PaaS systems. |
| **Kenya Data Protection Act (DPA) 2019** *(if local)* | Local data privacy regulation aligning with GDPR. | Governs how citizen data is collected, stored, and processed locally or in the cloud. |
| **PCI-DSS** *(If payment gateways are integrated)* | Payment Card Industry Data Security Standard. | Required for any M-PESA/mobile money integrations or online billing portals. |
| **CAK (Communications Authority of Kenya) Regulations** *(if applicable)* | Local telecom sector compliance. | Regulates lawful intercept, SIM registration, and secure communications. |

**2. Compliance Integration in Cloud Migration Phases**

| **Phase** | **Compliance Actions** |
| --- | --- |
| **Initiation & Planning** | Conduct Data Protection Impact Assessment (DPIA). Identify regulated data types. Engage compliance/legal team. |
| **Design & Architecture** | Choose cloud regions to meet data residency (e.g., EU or Africa-based data centers). Embed privacy-by-design principles. |
| **Migration Execution** | Apply encryption-in-transit and at-rest. Use role-based access control (RBAC) and audit trails. |
| **Post-Migration Validation** | Perform compliance audits (ISO 27001 readiness checks, GDPR assessments). Ensure backup, retention, and deletion policies align with DPA/GDPR. |
| **Operations & Monitoring** | Continuously monitor data access logs, breach reporting SLAs, and third-party vendor compliance. |

**3. Roles and Responsibilities**

| **Role** | **Responsibility** |
| --- | --- |
| **IT Project Manager** | Track compliance tasks, maintain documentation, and coordinate audits. |
| **Legal/Compliance Officer** | Interpret regulatory requirements and verify controls are enforced. |
| **Cloud Service Provider** | Ensure platform-level compliance (e.g., provide ISO 27001 certified infrastructure). |
| **Security Officer** | Implement technical controls—encryption, identity management, monitoring. |

**4. Documentation & Audit Readiness**

* Maintain:
  + Data processing records
  + Consent forms and policies (if applicable)
  + DPIAs and risk assessments
  + Vendor compliance certifications (SOC 2, ISO 27001)
* Prepare for:
  + Audits by internal and external stakeholders
  + Regulatory authority investigations (GDPR, DPA, CAK)

**5. Tools and Tracking Mechanisms**

| **Tool** | **Purpose** |
| --- | --- |
| **Compliance Tracking Sheets** | Track fulfillment of each regulatory clause. |
| **Audit Logs** | Generated from cloud services (AWS CloudTrail, GCP Audit Logs, etc.). |
| **Risk Register** | Includes legal and compliance-related risks with mitigation actions. |