**Data Governance Framework**

**1. Governance Structure**

A well-defined governance structure ensures accountability and adherence to data management policies. The key roles and responsibilities include:

**Key Roles & Responsibilities:**

* **Chief Data Officer (CDO):** Oversees the overall data strategy, ensures data quality, and enforces governance policies.
* **Chief Information Security Officer (CISO):** Manages data security, implements risk mitigation strategies, and ensures compliance with regulations.
* **Compliance Manager:** Ensures all data policies align with legal and regulatory requirements.
* **Data Stewards (Domain-Specific):** Manage data integrity, classification, and quality for their respective domains.

**2. Data Classification**

Data classification is crucial for risk management and ensuring appropriate data handling. The organization classifies data into four categories:

1. **Public Data:**
   * Non-sensitive information that can be shared publicly.
   * Examples: Marketing materials, public financial reports.
2. **Internal Data:**
   * Restricted to internal organizational use.
   * Examples: Internal project documents, organizational policies.
3. **Confidential Data:**
   * Contains sensitive business or customer financial information.
   * Examples: Bank account details, contract agreements.
4. **Highly Sensitive Data:**
   * Personal identification details and transactional records.
   * Examples: Social Security numbers, credit card details, personally identifiable information (PII).

**3. Data Lifecycle Management**

Managing data throughout its lifecycle ensures compliance, security, and efficient storage management.

**3.1 Data Creation**

* Data must be collected using validated input mechanisms to ensure accuracy and completeness.
* All input data should undergo verification before storage.

**3.2 Data Storage**

* All stored data must be encrypted using industry-standard encryption techniques.
* Segregation of data based on classification to prevent unauthorized access.

**3.3 Data Access**

* Strict **Role-Based Access Control (RBAC)** is implemented to grant access based on user roles and responsibilities.
* Multi-factor authentication (MFA) is required for access to sensitive data.

**3.4 Data Retention**

Data must be retained based on compliance and operational needs:

* **Transaction Records:** Retained for **7 years**.
* **Customer Records:** Retained for **10 years post-account closure**.
* **Loan Documents:** Retained for the **life of the loan + 7 years**.

**3.5 Data Archival & Disposal**

* Data that is no longer required is securely archived or permanently deleted using secure data disposal methods.
* Highly sensitive data must be shredded or digitally wiped beyond recovery.

**4. Compliance & Monitoring**

* Regular audits and monitoring are conducted to ensure adherence to data governance policies.
* Automated tools are used to track data access and modifications.
* Data breaches and policy violations must be reported immediately to the CISO and Compliance Manager.

This Data Governance Framework ensures the secure, compliant, and efficient handling of organizational data while protecting sensitive information and maintaining regulatory adherence.