**Data Governance Framework**

**1. Governance Structure**

A robust governance structure ensures accountability, quality, and compliance across the organization’s data assets.

**Key Roles & Responsibilities:**

* **Chief Data Officer (CDO)**
  + Owns the data strategy and governance implementation.
  + Aligns data policies with business goals.
  + Leads the Data Governance Council.
* **Chief Information Security Officer (CISO)**
  + Oversees data security and risk management.
  + Defines cybersecurity protocols for data protection.
* **Compliance Manager**
  + Ensures data usage aligns with regulatory requirements (e.g., GDPR, CCPA).
  + Monitors audits and compliance reporting.
* **Data Stewards (per domain)**
  + Manage data quality and integrity in their specific data domain (e.g., Finance, Sales, HR).
  + Define data definitions, standards, and resolve data issues.

**2. Data Classification**

Data is categorized based on sensitivity and intended use to guide appropriate security, sharing, and handling practices.

| **Classification** | **Description** | **Examples** |
| --- | --- | --- |
| **Public Data** | Non-sensitive; freely distributable | Marketing brochures, public web content |
| **Internal Data** | Limited to internal use; not for public release | Business emails, internal training materials |
| **Confidential Data** | Sensitive; access restricted to roles | Customer financial data, internal reports |
| **Highly Sensitive Data** | Strictest controls due to legal/regulatory risk | Personally Identifiable Info (PII), transaction logs |

**🔄 3. Data Lifecycle Management**

Proper data lifecycle controls ensure integrity, security, and compliance from data creation to deletion.

**Lifecycle Phases:**

* **Creation**
  + Data entered via validated input forms and automated data pipelines.
  + Validation rules enforced at the source.
* **Storage**
  + Data stored in encrypted formats (AES-256).
  + Segregation of environments (production, dev, test).
  + Redundancy and backup policies in place.
* **Access**
  + Enforced **Role-Based Access Control (RBAC)**.
  + Logging and monitoring of all data access events.
  + MFA for privileged users.
* **Retention**

| **Data Type** | **Retention Policy** |
| --- | --- |
| Transaction Records | Retained for **7 years** |
| Customer Records | Retained for **10 years** post-account closure |
| Loan Documents | Retained for **life of loan + 7 years** |

* **Archival & Disposal**
  + Archived to secure cold storage when inactive.
  + Disposal follows secure deletion protocols (e.g., DoD 5220.22-M).