**Task 4**

**Data Governance Framework**

**1. Governance Structure**

Effective data governance requires a clearly defined structure to ensure accountability, compliance, and data integrity. The governance structure consists of the following roles and responsibilities:

* **Chief Data Officer (CDO):**
  + Owns the organization’s data strategy and governance framework.
  + Leads data policy implementation and ensures alignment with business goals.
* **Chief Information Security Officer (CISO):**
  + Ensures data security policies are enforced.
  + Oversees risk management and security compliance related to data assets.
* **Compliance Manager:**
  + Ensures adherence to relevant laws, regulations, and standards (e.g., GDPR, RBI, HIPAA).
  + Coordinates audits and manages regulatory reporting.
* **Data Stewards (per domain):**
  + Maintain data quality, accuracy, and consistency across business domains.
  + Act as domain experts and support the enforcement of data standards and policies.

**2. Data Classification**

To ensure appropriate handling and protection, all organizational data is categorized as follows:

| **Classification** | **Description** | **Example** |
| --- | --- | --- |
| **Public Data** | Non-sensitive information available for public use | Marketing materials, website content |
| **Internal Data** | Restricted to internal stakeholders | Internal memos, internal reports |
| **Confidential Data** | Sensitive business data requiring protection | Customer financial information |
| **Highly Sensitive Data** | Personally Identifiable Information (PII) and regulated data | Transaction details, Aadhaar numbers |

**3. Data Lifecycle Management**

A comprehensive lifecycle approach ensures data is managed securely from creation to deletion.

**3.1. Creation**

* Use validated and standardized data entry mechanisms.
* Enforce input validation and data integrity checks at the source.

**3.2. Storage**

* All data stored in encrypted formats (at rest and in transit).
* Segregated storage zones for different data sensitivity levels.

**3.3. Access**

* Enforce **Role-Based Access Control (RBAC)**.
* Regular audits and reviews of access permissions.
* Multi-factor authentication for sensitive data access.

**3.4. Retention**

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