**Task:4 Data Governance Framework**

**Objective:**

The objective of this task is to create a comprehensive Data Governance Framework document that defines the governance structure, data classification, and data lifecycle management within an organization. This framework ensures that data is managed consistently, securely, and in compliance with regulations.

**1. Governance Structure**

The governance structure establishes accountability and responsibility for data management within the organization. Key roles include:

1. **Chief Data Officer (CDO):**
   * Owns and oversees the organization's data strategy.
   * Ensures data management aligns with business goals.
2. **Chief Information Security Officer (CISO):**
   * Manages data security and protection strategies.
   * Ensures compliance with security regulations and standards.
3. **Compliance Manager:**
   * Ensures compliance with regulatory requirements.
   * Monitors data governance policies.
4. **Data Stewards (Per Domain):**
   * Responsible for data quality, classification, and lifecycle management.
   * Ensures data accuracy and consistency.

**2. Data Classification**

Data classification categorizes data based on its sensitivity and impact on the organization. This helps determine appropriate security measures and handling procedures.

1. **Public Data:**
   * Non-sensitive information intended for public use.
   * Examples: Marketing material, public reports.
2. **Internal Data:**
   * Information for internal use only; not publicly available.
   * Examples: Internal emails, company procedures.
3. **Confidential Data:**
   * Sensitive data requiring protection to prevent harm.
   * Examples: Customer financial information, employee records.
4. **Highly Sensitive Data:**
   * Critical data requiring the highest security.
   * Examples: Personal identification, financial transactions, proprietary algorithms.

**3. Data Lifecycle Management**

Data Lifecycle Management (DLM) defines how data is managed throughout its lifecycle, from creation to deletion.

1. **Creation:**
   * Validated input mechanisms to ensure data accuracy.
   * Data is classified upon creation.
2. **Storage:**
   * Data is stored securely with encryption and segregation.
   * Periodic audits ensure data integrity.
3. **Access:**
   * Strict Role-Based Access Control (RBAC) ensures data is accessible only to authorized users.
   * Multi-factor authentication (MFA) for sensitive data.
4. **Retention:**
   * 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.
5. **Disposal:**
   * Secure data destruction methods to prevent recovery.
   * Compliance with legal and regulatory requirements.

**Conclusion:**

A robust Data Governance Framework ensures data is consistently managed, securely stored, and appropriately accessed throughout its lifecycle. This framework helps organizations mitigate risks, ensure compliance, and derive maximum value from their data assets.