**Step 1: Understand the Task and Goals**

* Task Objective: You need to create a Data Governance Framework document outlining the governance structure, data classification, and data lifecycle management.

**Step 2: Create a Governance Structure**

* **Define the Key Roles and Responsibilities:**
  1. **Chief Data Officer (CDO):** Responsible for overseeing data strategy, governance, and data management processes.
  2. **Chief Information Security Officer (CISO):** Ensures the security of data, particularly sensitive data.
  3. **Compliance Manager:** Ensures that data governance adheres to legal and regulatory standards.
  4. **Data Stewards:** Appoint individuals for each domain who are responsible for maintaining and overseeing data quality and standards.
* **Document the Governance Hierarchy:**
  1. Outline the reporting structure and decision-making framework.
  2. Ensure that roles and responsibilities are clearly defined.

**Step 3: Define Data Classification**

* **Classify Data Based on Sensitivity:**
  1. **Public Data:** Non-sensitive information available for public access. (e.g., company brochures, public reports)
  2. **Internal Data:** Restricted to the organization’s internal use, not for public release. (e.g., internal emails, internal reports)
  3. **Confidential Data:** Customer-related data such as financial details that require protection. (e.g., customer contact information, transactional data)
  4. **Highly Sensitive Data:** Extremely sensitive information, requiring the highest level of security. (e.g., personal identification information, medical data, credit card details)
* **Create Classification Guidelines:**
  1. Develop guidelines on how each data category should be handled, including access restrictions, encryption, and sharing protocols.

**Step 4: Define Data Lifecycle Management**

* **Create a Detailed Data Lifecycle Process:**
  1. **Creation:**
     + Ensure that all data entered into the system is validated (e.g., using forms with validation rules or automated checks).
  2. **Storage:**
     + Use encrypted storage mechanisms and separate storage areas for different data classifications.
  3. **Access:**
     + Implement **Role-Based Access Control (RBAC)** to ensure only authorized individuals can access sensitive data.
  4. **Retention:**
     + Define retention policies based on data type:
       - **Transaction records:** Retain for 7 years.
       - **Customer records:** Retain for 10 years post-account closure.
       - **Loan documents:** Retain for the life of the loan plus 7 years.
* **Establish Retention and Deletion Policies:**
  1. Create policies and processes for data retention and secure deletion once data is no longer needed.

**Step 5: Develop Policies and Procedures**

* **Create Documentation for Data Governance Policies:**
  + Develop internal policies covering:
    1. Data access rules
    2. Data handling and storage standards
    3. Data protection protocols (encryption, access control)
    4. Data retention and deletion practices
    5. Compliance standards and legal requirements
* **Data Access Control Policy:**
  + Define who has access to which types of data.
  + Use tools like RBAC to automate and enforce access control.
* **Data Security and Compliance Procedures:**
  + Document the procedures for data encryption, data masking, and secure data transmission.
  + Ensure alignment with industry standards like **GDPR** (General Data Protection Regulation) or **CCPA** (California Consumer Privacy Act) if applicable.

**Step 6: Implement Data Governance Tools and Systems**

* **Select Tools for Data Governance:**
  + Choose software or platforms for data governance that support:
    1. **Data Classification and Cataloging**
    2. **Data Access Management (RBAC)**
    3. **Data Quality Monitoring**
    4. **Audit and Compliance Reporting**
* **Implement Data Stewardship Processes:**
  + Appoint data stewards for each data domain (e.g., financial data, customer data) to ensure proper oversight and management of data quality.

**Step 7: Monitor and Evaluate Data Governance Practices**

* **Track and Audit Data Access and Usage:**
  + Regularly audit who is accessing what data and whether the security policies are being adhered to.
  + Ensure that data usage is aligned with the classification and access controls in place.
* **Regular Reviews and Updates:**
  + Regularly review data governance policies and procedures to ensure they remain relevant and up-to-date.
  + Update policies when there are changes in data regulations or organizational requirements.

**Step 8: Create a Report and Final Documentation**

* **Compile All Information into a Final Data Governance Document:**
  + Document the governance structure, classification, lifecycle management policies, and security measures.
  + Include detailed procedures for compliance, security, and access control.
* **Finalize and Distribute the Document:**
  + Once completed, distribute the document to relevant stakeholders for review and approval.
  + Ensure proper training for employees on how to implement and follow the data governance framework.

**Step 9: Ongoing Review and Improvement**

* **Establish a Process for Continuous Improvement:**
  + Continuously monitor data governance performance and make improvements based on feedback, audits, and any emerging challenges.