**Data Governance Framework**

**Governance Structure :**

Effective data governance is crucial to ensure the integrity, availability, and security of data within an organization. The following structure outlines the roles and responsibilities involved in managing the data governance framework.

**1. Data Ownership:**

**Chief Data Officer (CDO)**

* Overall responsibility for the organization's data strategy, policies, and governance.
* Ensures alignment between data initiatives and business objectives.
* Acts as the highest authority for data-related decisions across the organization.

**Chief Information Security Officer (CISO)**

* Ensures data security and compliance with privacy regulations.
* Responsible for the protection of sensitive data and overseeing access control mechanisms.
* Works with the CDO to establish data security policies and enforcement.

**Compliance Manager**

* Ensures that the organization complies with data regulations, laws, and standards.
* Monitors adherence to legal and regulatory requirements, including data protection laws (GDPR, CCPA, etc.).
* Collaborates with CDO and CISO to develop strategies for compliance management.

**Data Stewards for Each Domain**

* Designated individuals responsible for managing data quality, consistency, and standardization within specific domains (e.g., finance, sales, HR).
* Ensure that the data within their domain adheres to governance policies and supports organizational goals.
* They serve as the point of contact for data issues, quality concerns, and improvements within their domain.

**Data Classification**

Data classification is the process of categorizing data based on its sensitivity and the level of protection required. The following categories outline the classification for different types of data:

* 1. **Public Data:**
* **Definition**: Non-sensitive information that can be made publicly available without any risk to the organization or individuals.
* **Examples**: Marketing materials, press releases, product descriptions, and publicly available research.
* **Handling**: Public data can be freely shared with minimal restrictions. No special protection or encryption is required.
  1. **Internal Data:**
* **Definition**: Restricted organizational data intended for internal use only, not meant to be shared outside the organization.
* **Examples**: Internal emails, policies, internal memos, and project documentation.
* **Handling**: Restricted to employees and authorized personnel. It is managed under access control policies and may be subject to encryption depending on its sensitivity.
  1. **Confidential Data:**
* **Definition**: Sensitive data that could have an impact on the organization or its customers if exposed. This data is not to be disclosed to unauthorized parties.
* **Examples**: Customer financial information, employee salary data, business contracts.
* **Handling**: Access is restricted to authorized personnel only. Data should be encrypted and stored in secure locations. Strict access controls must be in place.
  1. **Highly Sensitive Data:**
* **Definition**: Data that could lead to severe consequences if disclosed, such as personal or private information about individuals.
* **Examples**: Personally Identifiable Information (PII), transaction details, medical records, passwords, credit card numbers.
* **Handling**: Highest level of security. Must be encrypted during storage and transit. Access is granted on a need-to-know basis, and multi-factor authentication should be required for access.

**Data Lifecycle Management :**

Data lifecycle management ensures that data is properly created, stored, accessed, retained, and disposed of in a secure and compliant manner.

* 1. **Creation:**
* **Validated Input Mechanisms**: Ensure that data is entered correctly and consistently from the start. Input validation checks must be in place to ensure the data's integrity.
* **Data Quality Standards**: Establish clear standards for what constitutes high-quality, accurate, and valid data upon creation.
  1. **Storage:**
* **Encrypted Storage**: Sensitive data, such as financial records or customer information, must be encrypted in storage using industry-standard encryption methods (e.g., AES-256).
* **Segregated Storage**: Store sensitive data in separate, protected environments to reduce the risk of unauthorized access.
* **Cloud vs On-premise**: Ensure that whether using cloud storage or on-premise, all storage complies with data security and privacy requirements.
  1. **Access:**
* **Role-Based Access Control (RBAC)**: Implement RBAC policies to ensure that individuals can only access data necessary for their role. Access should be granted based on job responsibilities.
* **Audit Trails**: Maintain logs of data access to monitor for unauthorized access and usage. Regular audits should be conducted to ensure compliance with access controls.
  1. **Retention:**

Data retention policies ensure that data is kept for as long as necessary and disposed of securely once it is no longer needed.

* **Transaction Records**: Retain transaction records for **7 years** to comply with financial regulations and auditing requirements.
* **Customer Records**: Retain customer records for **10 years post-account closure** to allow for legal or regulatory investigations and to maintain the history of business relationships.
* **Loan Documents**: Retain loan documents for the **life of the loan + 7 years**, ensuring that all documentation is available for legal and financial audits.

**Archiving and Disposal**:

When data reaches the end of its retention period, it must be securely archived or disposed of in a way that ensures it cannot be recovered. This includes secure deletion methods and shredding physical records.

**Conclusion:**

The Data Governance Framework ensures that all organizational data is managed and protected in a structured, secure, and compliant manner. By establishing clear ownership, classification, and lifecycle management policies, an organization can ensure that data is an asset that supports its business objectives while mitigating risks associated with data security, privacy, and compliance.

This framework is essential for organizations aiming to maximize the value of their data while ensuring its protection and compliance with relevant laws and regulations.