**Data Governance Framework Document**

**1. Governance Structure**

**Roles & Responsibilities**

* **Chief Data Officer (CDO)**
  + Oversees enterprise-wide data strategy and governance
  + Ensures data quality and regulatory compliance
* **Chief Information Security Officer (CISO)**
  + Implements and monitors data security controls
  + Leads incident response for data breaches
* **Compliance Manager**
  + Ensures adherence to GDPR, CCPA, PCI-DSS and other regulations
  + Conducts periodic compliance audits
* **Data Stewards (Domain-Specific)**
  + Finance Data Steward
  + Customer Data Steward
  + Transaction Data Steward
  + Product Data Steward  
    *(Each responsible for data quality in their domain)*

**2. Data Classification**

**Classification Levels**

1. **Public Data**
   * Non-sensitive information (e.g., marketing materials, public reports)
   * Accessible to all employees and external parties
2. **Internal Data**
   * Business-sensitive information (e.g., internal policies, operational metrics)
   * Restricted to employees and authorized contractors
3. **Confidential Data**
   * Customer financial information (e.g., account balances, transaction history)
   * Requires explicit authorization for access
4. **Highly Sensitive Data**
   * Personal identification (e.g., SSNs, biometric data)
   * Transaction details and authentication credentials
   * Strictest access controls with multi-factor authentication

**3. Data Lifecycle Management**

**A. Data Creation**

* **Validated Input Mechanisms**
  + Automated data validation rules at point of entry
  + Mandatory metadata tagging for all new data

**B. Data Storage**

* **Encrypted Storage**
  + AES-256 encryption for data at rest
  + Geographically distributed storage with failover
* **Segregation**
  + Logical separation by classification level
  + Physical separation for highly sensitive data

**C. Data Access**

* **Role-Based Access Control (RBAC)**
  + Predefined roles with least-privilege principles
  + Quarterly access reviews and recertification
* **Monitoring**
  + Real-time logging of all data access attempts
  + Behavioural analytics for anomaly detection

**D. Data Retention & Disposal**

* **Retention Periods**
  + Transaction records: **7 years** (regulatory minimum)
  + Customer records: **10 years post-account closure**
  + Loan documents: **Life of loan + 7 years**
  + Marketing data: **3 years from last interaction**
* **Secure Disposal**
  + Cryptographic erasure for digital data
  + Physical destruction of storage media

**4. Implementation Roadmap**

**Phase 1 (0-3 Months)**

* Appoint data stewards
* Implement initial classification system

**Phase 2 (3-6 Months)**

* Deploy RBAC framework
* Establish data quality metrics

**Phase 3 (6-12 Months)**

* Automate lifecycle management
* Conduct organization-wide training

This framework ensures **regulatory compliance, data integrity, and optimal data utility** while minimizing risk