Data Governance Framework

Data Governance Framework

Data Governance Framework for ADPA (Advanced Document Processing & Automation)

This framework aligns with DMBOK 2.0 principles and addresses the specific needs of the ADPA project, focusing on the data generated, managed, and processed within the system. It emphasizes a shared responsibility model, practical implementation, transparency, and continuous improvement.

1. Introduction & Purpose:

This framework defines the governance structure, policies, and processes for managing data within the ADPA ecosystem. Its purpose is to ensure data quality, security, compliance, and efficient use of resources. The framework's success relies on the active participation and collaboration of all roles defined herein.

2. Scope:

This framework covers all data generated, processed, and stored by ADPA, including:

- **Generated Data:** Documents (Project Charters, Business Cases, Requirements Documents, Data Governance Frameworks, etc.), reports, and analytics.
- **Source Data:** User inputs, template data, and external data sources (if integrated).
- **Metadata:** Data lineage, timestamps, user IDs, AI provider used, template versions, and other relevant contextual information.
- **Configuration Data:** API keys, connection strings, system settings, and user roles/permissions. This will likely be managed separately via a secrets management system in a production environment.

3. Governance Structure:

A three-tiered governance structure is implemented:

- **Data Governance Council (DGC):** A senior-level cross-functional committee responsible for strategic oversight, policy approval, resource allocation, and conflict resolution. Members will include representatives from IT, Business Analysis, Project Management, and Legal/Compliance.

- **Data Owners:** Business leaders responsible for the data within their respective domains (e.g., Project Management, Business Analysis). They define business rules, ensure data quality, and authorize access.

- **Data Stewards:** Subject matter experts (SMEs) responsible for the daily management of specific data domains. They ensure data

quality, enforce policies, and act as primary contacts for data-related questions. Examples include:

- **Template Steward:** Manages document templates, ensuring compliance with relevant standards (BABOK, PMBOK).
- **Security Steward:** Manages security aspects, including API keys and access control.
- **Metadata Steward:** Ensures consistent metadata capture and reporting.

- **Data Custodians:** The IT/DevOps team responsible for the technical infrastructure (databases, storage, etc.). They are responsible for data security, backups, and disaster recovery.

4. RACI Matrix: (Responsibility Assignment Matrix) This clarifies roles for key data activities.

Activity	DGC	Data Owner	Data Steward	Data Custodian
Policy Definition/Approval	A	I	C	I
Template Approval	A	I	R	I
Data Quality Rule Definition	A	I	R	I
Data Security Implementation	A	I	C	R
Issue Resolution	A	R	R	R
Data Breach Response	A	R	I	R

Activity	DGC	Data Owner	Data Steward	Data Custodian
Metadata Standard Definition	A	I	R	I
Data Retention Policy	A	I	C	R

5. Data Policies and Standards:

- **Template Governance Policy:** All templates must be version-controlled, reviewed, and approved before deployment. Metadata must be included (name, version, description, standard reference).

- **Data Security & Access Control Policy:** Access is granted based on the principle of least privilege. Sensitive data (API keys, credentials) are managed securely (e.g., Azure Key Vault). Authentication and authorization are enforced on all API endpoints.

- **Metadata Management Policy:** All generated data includes standardized metadata (document ID, template ID, timestamp, user ID, AI provider). Metadata is consistently captured and reported.

- **Data Quality Policy:** Defines standards for data accuracy, completeness, consistency, timeliness, and validity. Includes processes for identifying and resolving data quality issues.

- **Data Retention & Lifecycle Policy:** Defines retention periods for different data types (documents, logs, templates). Includes procedures for archiving and disposal.

6. Decision Rights and Escalation:

- **Operational Issues:** Data Stewards resolve. Escalate to Data Owners if needed, then DGC.
- **Policy Exceptions:** Data Stewards make recommendations; DGC approves.

- **Template Approval:** Data Steward proposes; Data Owner and DGC approve.
- **Data Quality Issues:** Data Stewards resolve. Escalate to Data Owners and/or DGC for significant issues.
- **Data Security Issues:** Data Custodians and Security Steward address; escalate to DGC if major.

7. Compliance and Regulatory Alignment:

The framework ensures compliance with relevant regulations (GDPR, SOX, HIPAA, PCI DSS). Policies and procedures are designed to meet these requirements.

8. Monitoring and Continuous Improvement:

- **Regular Reporting:** Key metrics (policy adherence, data quality, issue resolution time) are tracked and reported to the DGC.
- **Regular Reviews:** The framework is reviewed and updated annually or as needed to adapt to changing requirements and business needs. Data Steward syncs and DGC meetings facilitate this process.
- **Feedback Mechanisms:** Regular feedback channels (e.g., surveys, issue tracking) are established to gather input for continuous improvement.

9. Training and Awareness:

Training programs will be developed and delivered to all relevant personnel to ensure understanding and adherence to the framework's policies and procedures.

This Data Governance Framework provides a robust structure for managing data within the ADPA project, ensuring its quality, security, and compliance with relevant standards and regulations. Its success depends on the active involvement and commitment of all stakeholders.