Data Governance Plan

> **Source File:** generated-documents\dmbok\data-governance-plan.md
> **Generated:** 16/07/2025 at 13:56:33
> **Generated by:** Requirements Gathering Agent - PDF Converter

Data Governance Plan

Generated by adpa-enterprise-framework-automation v3.2.0
Category: dmbok
Generated: 2025-07-15T18:35:59.027Z
Description: Comprehensive plan outlining data governance objectives, principles, roles, responsibilities, and processes in alignment with DMBOK best practices.

Data Governance Plan

Project: ADPA – Advanced Document Processing & Automation Framework
Version: 3.2.0
Prepared by: Data Governance Lead
Date: [Insert Date]

---

1. Introduction

1.1 Purpose and Scope

This Data Governance Plan establishes a comprehensive framework for managing data assets within the ADPA (Advanced Document Processing & Automation Framework) project. ADPA is a modular, standards-compliant Node.js/TypeScript framework for AI-powered document generation, project management, and business analysis, supporting enterprise integrations (Confluence, SharePoint, Adobe, etc.) and complying with BABOK v3, PMBOK 7th Edition, and DMBOK 2.0.

This plan is designed to:

- Ensure high data quality and integrity across all ADPA modules and integrations.
- Support regulatory and industry compliance (GDPR, SOX, PCI DSS, FINRA, Basel III, etc.).
- Align with DMBOK 2.0 principles and enterprise objectives for secure, scalable, and effective data management.

1.2 Alignment with DMBOK and Organizational Objectives

ADPA's data governance aligns with DMBOK 2.0 by:

- Defining clear data stewardship and ownership.
- Establishing robust data quality, privacy, and security controls.
- Enabling enterprise-wide data integration, standardization, and compliance.
- Supporting continuous improvement and auditability.

---

2. Governance Structure

2.1 Roles & Responsibilities

Role	Responsibilities
Data Governance Council	Strategic oversight, policy approval, escalation of governance issues.
Chief Data Officer (CDO)	Executive accountability, regulatory compliance, risk management.
Data Stewards	Daily data quality, metadata management, access authorization, stewardship of specific domains (e.g., documents, templates, user data, audit logs).
System/Data Owners	Accountability for business data assets, stewardship assignment, data lifecycle decisions.
Data Custodians (IT)	Technical controls, data storage, backup, disaster recovery, infrastructure security.
Solution Architects	Ensure data models and APIs comply with governance standards.
Integration Leads	Ensure external system integrations (SharePoint, Confluence, Adobe, AI providers) comply with governance and security requirements.
End Users	Adhere to data usage, privacy, and security policies.

2.2 Committees and Escalation Paths

- **Data Governance Council:**
  Meets quarterly, reviews policies, resolves escalated issues.

- **Data Quality Committee:**
  Monitors and remediates cross-functional data quality issues.
- **Escalation:**
  Non-compliance or unresolved data issues are escalated from Data Stewards → Data Governance Council → CDO.

---

3. Data Policies, Standards, and Procedures

3.1 Key Data Policies

- **Data Classification:**
  All data (including generated documents, templates, configurations, user data, and audit logs) is classified as:
  - *Confidential*: User credentials, auth tokens, audit logs.
  - *Internal*: Generated business documents, templates, analytics.
  - *Public*: Open-source code, documentation.
- **Data Retention:**
  - Generated and stored documents: 7 years (unless superseded by client policy).
  - Authentication logs: 1 year.
  - Audit logs: 3 years.
  - Configuration files: Indefinite, with version control.
- **Access Control:**
  - Role-based access (RBAC) enforced for all interfaces (API, CLI, Web).
  - OAuth2, SAML, Active Directory integration for enterprise deployments.
  - Principle of Least Privilege (PoLP).
- **Data Privacy & Protection:**

    - All personal data handled per GDPR, CCPA, and relevant regulations.
    - Data encryption in transit (TLS 1.2+) and at rest (AES-256).
    - Anonymization and pseudonymization for analytics and reporting data.

- **Data Security:**
    - Secure API endpoints (JWT, API keys).
    - Regular vulnerability scanning and penetration testing.
    - Use of secure development practices (OWASP top 10).

- **Data Quality:**
    - Templates and generated documents must conform to business and regulatory standards (BABOK, PMBOK, DMBOK).
    - Validation, completeness, and consistency checks for all input/output.

3.2 Standards

- **Metadata Standards:**
    - All documents, templates, and data objects tagged with version, author, timestamp, and classification.
- **Naming Conventions:**
    - Standardized naming for templates, documents, and APIs (snake_case for files, camelCase for variables).
- **Documentation Standards:**
    - All data assets documented in the project's documentation repository and/or enterprise knowledge base (e.g., Confluence).

3.3 Procedures

- **Data Lifecycle Management:**
    - Clear onboarding, change management, archival, and deletion processes for all data types.
- **Incident Response:**

    - Data breaches are reported to the CDO and Data Governance Council within 24 hours.
    - Root cause analysis and remediation procedures in place.
- **Change Control:**
    - All changes to data-related code or configurations reviewed and approved through GitHub pull requests and change control board.
- **Backup & Recovery:**
    - Automated, encrypted backups of configuration, templates, and persistent data.
    - Disaster recovery drills tested bi-annually.

---

4. Data Stewardship and Ownership

4.1 Assignment of Stewards & Owners

- **Data Stewards:**
  Appointed for each major data domain (e.g., Document Templates, Generated Documents, User Data, Integration Metadata, Audit Logs).

- **System/Data Owners:**
  Typically product managers or business leads for each module or integration.

4.2 Stewardship Responsibilities

- Ensure data quality, completeness, and integrity within their domain.
- Maintain metadata and documentation for assigned assets.
- Monitor access and usage; enforce policies.
- Serve as point of contact for data-related questions and issues.
- Participate in data quality reviews and audits.

---

5. Compliance, Risk Management, and Audit

5.1 Regulatory & Compliance Requirements

- **Financial:** Basel III, MiFID II, FINRA, CFTC, FCA, BaFin.
- **Security:** GDPR, SOX, PCI DSS, ISO 27001/9001.
- **Healthcare (if applicable):** HIPAA.
- **Government (if applicable):** FedRAMP.

Compliance is mandatory for all modules, APIs, and integrations.

5.2 Risk Management Approach

- **Risk Identification:**
  Annual risk assessment for all data flows, integrations, and storage.
- **Mitigation Measures:**
  - Regular security reviews, code scanning, and dependency management.
  - Third-party risk due diligence for AI providers and SaaS integrations.
  - Data loss prevention (DLP) measures and monitoring.
- **Incident Management:**
  - Documented playbooks for incident response.
  - Root cause analysis and remediation tracking.

5.3 Audit & Review Processes

- **Internal Audits:**
  - Quarterly audits of data access logs, change histories, and compliance controls.
- **External Audits:**
  - Annual third-party audits for security and regulatory compliance (where contractually required).
- **Continuous Monitoring:**
  - Automated monitoring and alerting for policy violations, suspicious activity, and system health.

---

6. Communication and Training

6.1 Communication Plan

- Regular updates on data governance activities shared via Confluence, internal newsletters, and project meetings.
- Data governance documentation and standards published in the GitHub Wiki and Confluence.
- Escalation protocols and key contacts listed in onboarding materials.

6.2 Training & Awareness

- **Onboarding:**
  All new users and contributors receive data governance and security training.
- **Ongoing Training:**
  Annual refreshers on data policies, regulatory changes, and secure data practices.
- **Role-Based Training:**
  Stewards, owners, and developers receive advanced training on compliance, privacy, and quality procedures.

---

7. Metrics and Continuous Improvement

7.1 Key Metrics

- Data quality scores (completeness, accuracy, timeliness) for generated documents and templates.
- Number and severity of data incidents or policy violations.
- Audit findings and remediation rates.
- User access review frequency and exceptions.
- Training completion rates.

7.2 Continuous Improvement Processes

- Quarterly review of data policies, standards, and metrics for relevance and effectiveness.
- Stakeholder feedback mechanisms (via GitHub Discussions, Confluence, etc.).
- Dedicated budget and roadmap items for improving data governance (see project roadmap: DMBOK 2.0, advanced analytics, SSO, etc.).
- Lessons learned from incidents and audits incorporated into policy and practice updates.

---

8. Appendices

8.1 Glossary

- **Data Steward:** Person responsible for data quality in a specific domain.
- **Data Owner:** Business or technical lead responsible for the lifecycle and compliance of data assets.
- **DMBOK:** Data Management Body of Knowledge.
- **BABOK:** Business Analysis Body of Knowledge.
- **PMBOK:** Project Management Body of Knowledge.
- **RBAC:** Role-Based Access Control.
- **PoLP:** Principle of Least Privilege.

8.2 References

- DMBOK 2.0
- BABOK v3
- PMBOK 7th Edition
- ADPA Documentation
- Enterprise Compliance Standards

8.3 Supporting Documents

- ADPA Security Policy

- ADPA Change Management Process
- API and Integration Documentation
- Audit & Incident Response Playbooks

This Data Governance Plan is a living document and will be reviewed and updated at least annually or in response to material changes in project scope, regulations, or risk environment.
