



Maine State Government
Dept. of Administrative & Financial Services

Executive Branch Data Governance Policy

The Data Management Governance Practice (DMGP) has created the following Executive Branch Data Governance Policy for the Maine State government. This policy outlines governance over data quality, usability, and security, establishing a comprehensive framework for the collection, management, and use of data throughout the Executive Branch. It ensures compliance with relevant legislative and regulatory mandates and provides a foundation for high-quality data that supports operations, legislative and programmatic impact statements, financial decisions and investments, business systems, and reporting.

The goal of this policy is to establish a federated operating model that enhances partnership and communication among DMGP, agencies, bureaus, offices, divisions, and units, ensuring overall organizational efficiency and an improved constituent experience across the State of Maine.

This Executive Branch Data Governance Policy establishes a framework for exercising authority, control, and shared decision-making over data assets throughout their life cycle, from collection to disposal. It includes protocols for measurement, monitoring, and escalation if data quality is found deficient (e.g., incomplete, inaccurate, or irrelevant). Additionally, the Policy delineates the roles and responsibilities of various stakeholders involved in the sponsorship, management, and operations related to the collection, maintenance, integration, presentation, and consumption of data used in business processes.

These practices are crucial for ensuring that data is reliable, timely, accessible, and comprehensible, while also safeguarding it against unauthorized use and access. Data governance procedures will ensure that daily data management activities support the SOM's operations, decision-making, legislative, and regulatory compliance needs by providing complete, accurate, timely, and secure data.

Table of Contents

1.0 Overview	3
2.0 Purpose	3
3.0 Scope	3
4.0 Data Governance	4
5.0 Essential Components of the SOM Data Governance Framework.....	6
6.0 Data Governance Framework.....	10
7.0 Responsibility and Authority	11
7.1 Enterprise Data Council (EDC)	11
7.2 DMGP Working Groups	12
7.3 Agency Data Officer	13
7.4 Data Steward	14
7.5 Data Custodian.....	15
7.6 Organizational Change Management (OCM).....	17
8.0 Related Policies and Documents	18
9.0 Policy Governance and Approval	18
10.0 Review & Amendment.....	19
11.0 Data Governance Policy Document History	19
12.0 Appendix / Glossary of Terms.....	19

1.0 Overview

The State of Maine (SOM) recognizes that reliable, high-quality products, services, operations, and customer data are essential business assets. Proper governance and use of this data in daily operations are crucial to achieving strategic objectives, meeting customer expectations, documenting financial operations, analyzing legislative and programmatic impacts, and generating necessary reports. This Executive Branch Data Governance Policy delineates the enterprise roles and responsibilities of stakeholders involved in implementing the overall data governance framework.

2.0 Purpose

The objective of this policy is to establish and maintain a structured Data Governance framework that ensures appropriate decision-making and accountability in the creation, consumption, control, and valuation of SOM data and analytics. This policy delineates the roles, responsibilities, authority, and operations of the DMGP Working Group and Enterprise Data Council in support of the Data Governance practice.

This policy does not prescribe the standards and procedures for each represented group. Agency Data Officers will offer guidance, support, and mentoring to each business area to assist in defining the protocols for collecting and communicating essential information when engaging with respective stakeholders.

3.0 Scope

This policy applies to “the enterprise,” encompassing all SOM Executive Branch entities, including independent and quasi-independent agencies, and boards and commissions. It covers all data systems and sources created or maintained by MainIT, Executive Branch agencies, and their vendor partners.

In alignment with the enterprise policy, agencies shall define and maintain Data Governance frameworks consistent with this directive. Agencies shall establish and uphold their own Data Governance policies, along with any relevant procedures, processes, and metrics, to oversee and guide Data Governance activities at all levels. Such agency-level policies can be more proscriptive and detailed than this Policy but must align with the tenets outlined herein.

4.0 Data Governance

Data Governance involves organizing people, processes, and technology to effectively manage data as an important asset for an enterprise.

The Data Governance Institute describes data governance as “a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods.”

The Data Management Association International defines it as the “planning, oversight, and control over management of data and the use of data and data-related sources.”

Data Governance refers to policies relating to collection, access and use of data, while Data Management includes processes, tools, and enabling technology. To reflect this, the term “Data Governance Program” is expanded to the more comprehensive “Data Management and Governance Practice.” Both functions support the State of Maine’s cybersecurity posture.

Data Governance Guiding Principles and Objectives

The State of Maine’s Data Management and Governance Practice (DMGP) define data governance as the overarching organizational structures, processes, and technological tools that ensure data is managed as an asset. This ensures that data is complete, accurate, timely, and secure, while adhering to the following principles:

- The data used for operational processes, reporting, and regulatory compliance is continuously governed and managed.
- Data governance is integrated into relevant management systems and business processes, constituting a critical component of the enterprise’s internal control procedures.
- Successful management of data governance practices engages all personnel across the enterprise.

Data governance implementation at SOM is conducted iteratively through a phased approach. This method allows executive agencies to implement in manageable stages, increasing effectiveness in managing data across different organizational departments. The process is customized to align with the organization’s unique culture, facilitating gradual learning and adaptation for optimal success.

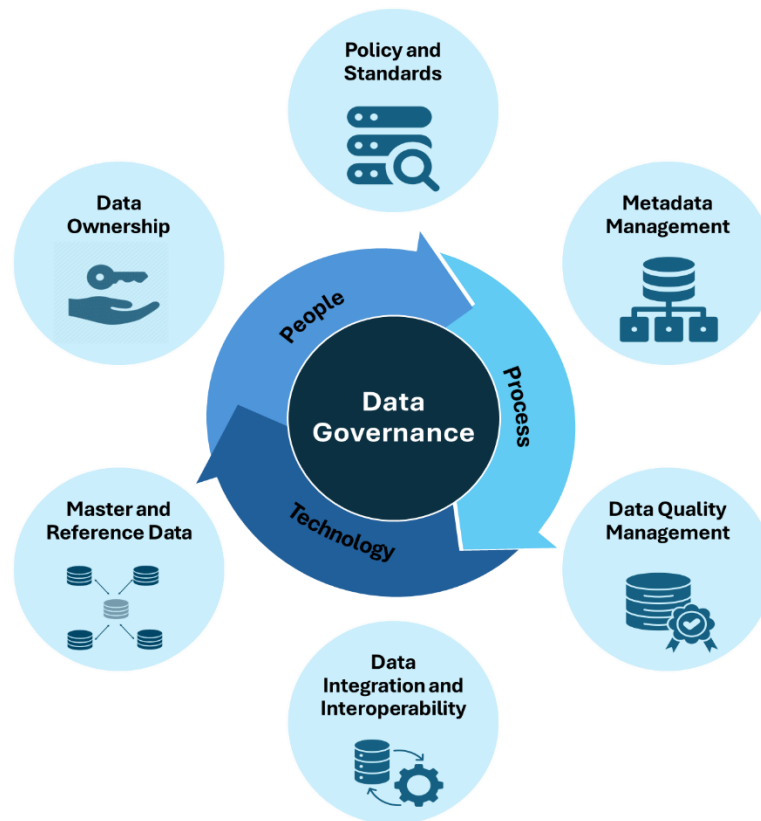
The principal objectives of data governance within the enterprise include ensuring data security, data quality, visibility, collaboration, data literacy, and expanded automation. It shall include the following:

- Governing enterprise data at SOM by treating it as an asset.
- Creating, guiding and maintaining data policies, standards, and processes to meet the requirements of data accuracy, consistency, conformity, timeliness, completeness, integrity, security, and privacy.
- Institutionalizing data governance roles and responsibilities by identifying and empowering Data Officers and Data Stewards for each agency to make key decisions about the data within their respective business area(s) and be accountable for those decisions.
- Establishing data catalogs with shared definitions, taxonomy, and associated vocabulary by documenting and maintaining data lineage and business and technical metadata.
- Standardizing data sharing through the use of a template and/or set of principles, so it is consistent between State agencies and external partners.
- Enabling consistent data usage and ensuring the quality and integrity of business-critical information.
- Addressing data synchronization systematically, reducing data redundancy, and improving data accessibility, availability, and flexibility.
- Establishing a source of truth for key domains and data elements.
- Automating and reconciling data management processes where possible and appropriate.
- Securing and managing sensitive data to prevent any data loss and tampering.
- Minimizing business and technical obstacles and silos to achieve the objectives of the business strategy.
- Providing a mechanism for open communication and transparency across multiple business areas and technical teams.
- Creating an innovative, data-driven environment through a culture of learning.
- Supporting opportunities to advance overall data solutions and innovation.
- Aligning personnel and processes to ensure data quality, managing and resolving issues at the root level, maintaining data privacy, utilizing data governance tools, and implementing change management and communication strategies.

5.0 Essential Components of the SOM Data Governance Framework

The SOM's data governance framework has adopted several key principles from the Data Management Association's Data Management Body of Knowledge (DAMA-DMBOK). This industry standard defines essential components of a data governance framework, which include:

- Policy and policy compliance (this document).
- Oversight, organizational structure, and roles.
- Standards and controls.
- Metadata, data quality management, and data integration.
- Master data management processes and systems.



The DMGP aims to provide the right data to the right people at the right time, supporting SOM's business operations and aligning it with business outcomes.

Data is crucial for decision-making at SOM. As a strategic asset, it should be effectively managed. The enterprise DMGP Program focuses on realizing the full value of data, with a vision that includes:

Data Ownership – Establishing accountability through designated data ownership. Data ownership involves taking responsibility for a specific set of data related to a particular domain within the agency. Agency Data Officers and Data Stewards are representatives from distinct business areas with extensive knowledge of their data needs and requirements. They have the authority to create, edit, modify, share, and control access to the data.

Policy and Standards - Establishing the Data Governance policy and standards, which are essential for the effective management and utilization of data within an organization. This policy and accompanying data standards provide a structured framework that delineates roles, responsibilities, and procedures for managing data as a valuable asset. By establishing data governance policy and standards, Executive Branch agencies can align their data management practices with business objectives, regulatory requirements, and industry best practices. This alignment fosters trust among stakeholders, enhances decision-making capabilities, and promotes transparency and accountability in data handling.

Data Standards will be created by DMGP in consultation with MaineIT and the Office of the Attorney General (OAG) (when appropriate) for specific data governance domains, such as Metadata Management (cataloging and formatting), Data Quality Management, lifecycle management, etc. Data Standards will serve as a companion to this policy and contain more detailed requirements, an example of which is the Data Sharing Agreement Guidelines. It contains technical requirements for security and privacy, as well as best practices for agencies to incorporate into the terms of their DSA's.

Future Data Standards will be added to a growing Enterprise Data Management Framework accessible to agency Data Stewards on the DMGP SharePoint site.

Metadata Management – Metadata is "data about data" that provides information about other data. Metadata management involves handling and organizing Metadata to ensure accessibility and comprehension for users. This process enables the creation of a catalog or inventory of data assets, facilitating easy discovery and retrieval of information. Additionally, metadata management establishes clear definitions to maintain consistency and understanding across an

organization. Effective metadata management can improve data discovery, data integration and interoperability, enhance data quality, ensure data compliance, and support informed decision-making.

Structuring and controlling data are essential to ensure its accuracy, integrity, consistency, and usability. Metadata management involves cataloging and overseeing data that details the technical and business characteristics, as well as the lineage, of the information.

Data Quality Management – This is the process of ensuring data accuracy, completeness, reliability, and relevance. It involves practices, standards, and technologies to maintain high data quality throughout its lifecycle. It verifies data against predefined criteria and business rules at entry or transfer and consolidates data from various sources for a unified view.

Effective data quality management ensures trustworthy data, crucial for informed decisions, operational efficiency, constituent experience, and regulatory compliance. Data quality and consistency can be improved by:

- Establishing a standard framework and standards for core data categories across agencies
- Setting metrics and key performance indicators (KPIs), consistently monitoring processes, and performing root cause analyses
- Identifying, selecting, and implementing data quality solutions

Data Integration and Interoperability – Data integration entails combining information from multiple sources to deliver a unified and comprehensive perspective. This process encompasses data consolidation, transformation, mapping, and synchronization.

Data interoperability refers to the capability of disparate systems and applications to communicate, exchange, and utilize data effectively. Achieving interoperability involves adopting common data standards, formats, protocols, and application programming interfaces (APIs), along with other mechanisms to facilitate interaction and data sharing. These practices ensure consistency and compatibility across various systems within the enterprise and among different agencies.

Data integration and interoperability are essential for facilitating seamless data exchange and collaboration across diverse systems, platforms, and agencies. By implementing robust data interoperability and integration practices, SOM can fully leverage its data, enhance operational efficiency, document impacts, and achieve improved outcomes.

DMGP provides guidance on integrating data from various sources with a unified view to ensure accuracy, consistency, accessibility, and the seamless exchange of information between systems and applications. The objective is to facilitate data sharing and comprehension across platforms without necessitating complex conversions.

Master and Reference Data Management – Master and reference data are critical types of data to maintain consistency, accuracy, and reliability of information.

Master data represents the key entities within the enterprise that are utilized across various business processes and systems. These entities are commonly shared and referenced by multiple departments and applications. Master data is essential for maintaining a single version of the truth, ensuring that all systems and processes refer to the same accurate data. Examples of master data include customers (patients, residents, clients), employees, and locations.

Reference data is a subset of master data consisting of static or slowly changing data used to categorize or classify other data within an organization. It provides context and meaning to transactional and master data. Reference data ensures consistency and standardization across different systems and processes by providing a common set of values for categorization and classification. Examples of reference data include country codes, state codes, budget codes, and tax identification numbers.

Effective management of master and reference data is crucial for maintaining data accuracy, consistency, and reliability across various systems and processes for SOM. The goal is to establish a single source of truth wherein one agency is the custodian of record for specific data and shares it with other agencies as needed and appropriate. This process entails mapping critical business processes to minimize data duplication and inconsistencies, streamlining operations, and enhancing data integration at the enterprise level. This reduces the number of times data needs to be collected to be used by multiple agencies.

By effectively managing master and reference data, SOM can improve data quality, enhance decision-making, and ensure smooth and efficient operations. Master and reference data establish a consolidated source of information that is independent of individual data sources, ensuring uniform and dependable data throughout the organization.

Sensitive Data Management – Sensitive data management involves collaborating with various agencies, along with privacy and InfoSec teams, to ensure the

protection and confidentiality of sensitive information such as Personally Identifiable Information (PII) and Protected Health Information (PHI). This process includes identifying and classifying sensitive data, implementing robust security measures, and continuously monitoring potential threats.

Effective sensitive data management not only safeguards critical information but also fosters trust and confidence among clients and partners by:

- Identifying and classifying sensitive data.
- Ensuring comprehensive controls for the sharing of both internal and external data.
- Enhancing standards and procedures to maintain data security and privacy.

Information Lifecycle Management – Implementing comprehensive data management practices to effectively control the capture, storage, access, and utilization of data and information across all forms or media. This is accomplished by:

- Establishing and enforcing an enterprise-wide policy for information lifecycle management, thereby ensuring the proper creation, storage, usage, retention, archiving, and secure disposal of data.

Repeatable Processes – Establishing consistent methods for managing data assets enterprise-wide.

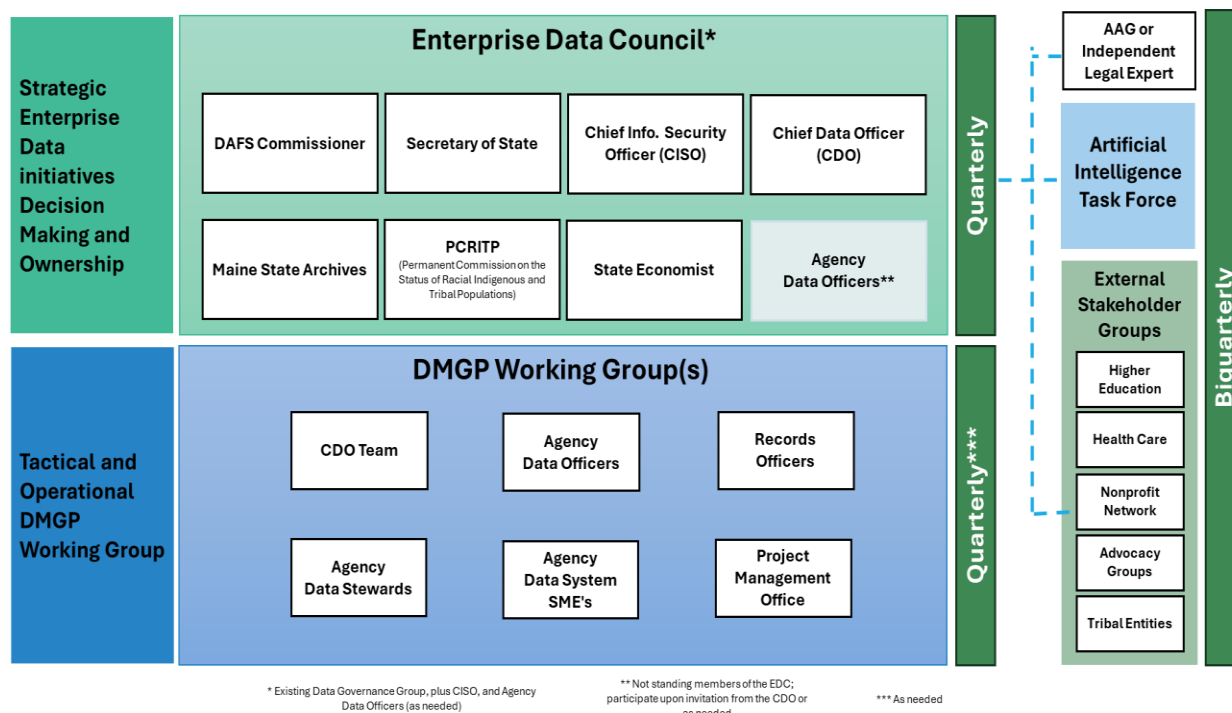
Collaboration – Working with various SOM agencies, divisions, bureaus, and MaineIT teams to:

- Provide guidance to reduce the number of duplicated data sources.
- Minimize manual data input, reconciliation and reporting efforts prone to errors.
- Achieve business value through collaboration and governance efforts.

6.0 Data Governance Framework

The SOM data governance framework features a two-tiered structure comprising members from state and independent agencies, as well as MaineIT, with clearly defined roles and responsibilities.

DMGP Federated Operating Model



7.0 Responsibility and Authority

The key roles and authority within the DMGP federated operating model include:

- Enterprise Data Council (EDC)
- DMGP Governance Workgroup(s)
- State Chief Data Officer (CDO)
- Agency Data Officers
- Agency Data Stewards

7.1 Enterprise Data Council (EDC)

The EDC at SOM is a diverse group of senior leaders dedicated to aligning enterprise-wide data objectives and guiding data governance initiatives within their respective business and functional areas.

EDC is responsible for guiding DMGP priorities, ensuring strategic alignment, driving consensus, and providing insight on the enforcement and monitoring of data policies, standards, procedures, requirements, and guidelines related to data management, data sharing, data access, data use, data privacy, data security, data quality, and data dissemination.

EDC serves as the governing authority for the State of Maine's DMGP, acting as a point of escalation for significant enterprise data decisions, issues, and risks.

High-Level Activities and Responsibilities:

- Aligns enterprise data requirements with statewide priorities, ensuring coherent data objectives.
- Ensures strategic alignment within their business and functional areas, fostering consensus and commitment to data management and governance initiatives.
- Provides guidance on the enforcement and monitoring of enterprise data policies, standards, procedures, requirements, and guidelines for data sharing, access, use, privacy, metadata, and quality.
- Recommends and reviews data governance policies, guidelines, and standards as necessary.
- Ensures resource alignment for data management and governance initiatives.
- Ensures the overall success of the Data Management and Governance Practice for the State of Maine.
- Collaborates with the External Stakeholder Group to inform statewide data initiatives.

7.2 DMGP Working Groups

The DMGP's Working Groups bear the primary responsibility for the execution and oversight of data governance activities. These workgroups focus on identifying and addressing data governance needs at the agency level, and are tasked with implementing standards, processes, and policies to achieve data management and governance objectives for their specific business areas. Furthermore, they are accountable for establishing and ensuring the effective operation of these processes throughout their organization.

High-Level Activities and Responsibilities:

- Ensures the implementation of data governance policies and standards across the entire enterprise, connecting all agency business areas, functional units, and MaineIT.
- Identifies and coordinates efforts between Data Stewards.
- Provides recommendations on data governance priorities to the Enterprise Data Council, as necessary.

- Communicates and oversees communication of data needs to the Data Stewards.
- Collaborates with Data Stewards to identify and resolve data issues at their root causes.
- Identifies potential opportunities for increased efficiency, improved data reuse, and enhanced data security and privacy.

7.3 Agency Data Officer

Agency Data Officers (DO) are senior leadership that oversee data governance at the agency level. They possess a high-level understanding of data needs and requirements within several key business areas. This distinction becomes necessary for State agencies with complexity and scale – multiple bureaus, offices, and divisions- but are not required for smaller agencies with narrower functions and mandates.

DOs advocate for data strategy and governance while assuming responsibility for the risks tied to business processes (service delivery, operations, program improvement, quality assurance, etc.) They provide guidance and direction to their Data Stewards and Data Custodians to coordinate their efforts and achieve consistency.

High-Level Activities and Responsibilities:

- Establishes and maintains guidelines aligned with enterprise data management and governance best practices, while advocating for the DG framework within the agency
- Accountable for maintaining data quality, safeguarding privacy, and ensuring security within their domain.
- Exercises statutory or operational authority over designated data.
- Responsible for establishing controls over data generation, collection, processing, access, dissemination, and disposal.
- Assumes high level responsibility for designated data assets, ensuring their definition, governance, quality, integrity, and alignment with enterprise guidelines, policies, and standards.
- Responsible for ensuring ownership & accountability (RACI) matrices for the data domain under their purview.

- Collaborates with the CDO and other agency Data Stewards to align agency technology procurement and requests for change with enterprise policies and standards.
- Responsible for overseeing business processes and data elements within their scope.
- Acts as the primary escalation point for Data Management and Governance issues within the business area.
- Establishes unified data requirements across the business area, ensuring optimal and intended data utilization.
- Empowers Data Stewards to address process and data issues within the business area while providing guidance on content direction.
- Reviews and approves appeals and exceptions; escalates to CDO and in rare cases to Enterprise Data Council.

7.4 Data Steward

Data Stewards at each agency are responsible for the day-to-day implementation of Data Management and Governance within their business unit(s). They are the backbone of data governance efforts at the agency level, ensuring adherence to standards, principles, and guidelines while implementing necessary controls and support mechanisms.

Recognized as Subject Matter Experts (SMEs), Data Stewards ensure data quality, promote privacy, enforce role and access controls, and coordinate with DOs to ensure alignment of their systems with agency and enterprise data management and governance policies and practices. Additionally, Data Stewards are advocates for the importance of data and governance within their respective business unit(s).

High-Level Activities and Responsibilities:

- Collaborates with the agency DO (if applicable) to provide expertise and data governance implementation within their respective business or functional area.
- Ensures adherence to Enterprise Data Management policies, standards, compliance, and data security within the designated business or functional area.
- Develops and maintains consistent data definitions, rules, and requirements, ensuring data quality, records management, and security across the business unit.

- Creates and manages data catalogs, business glossaries for functional areas, and application glossaries for source systems.
- Participates in cross-business unit collaboration to resolve issues related to data sharing, usage, quality, and security.
- Establishes data quality metrics/KPIs, conducts data validation and monitoring, and leverages standardized data cataloging and profiling tools and processes.
- Oversees and maintains data quality, data classification, data privacy and compliance objectives within the assigned functional area or domain.
- Guides data users in selecting the most suitable data sources and data custodians, providing informed recommendations and directions.
- Collaborates with the DMGP office to advance data management and governance practices while enhancing data literacy, organizational change management, and communication strategies.
- Enforces data standards, policies, and quality metrics while facilitating data sharing and master data management practices.
- Collaborates with business and Data Custodians to regularly assess and enhance Data Governance standards.
- Notifies data users of modifications in data requirements, structure, and usage while maintaining thorough documentation of updates.
- Supports the evaluation of change requests, assessing their disposition, implementation impacts, and potential alternatives.
- Identifies and reports the root causes of data quality, data privacy, and data security issues, escalating them appropriately when necessary.

7.5 Data Custodian

Data Custodian(s) are responsible for managing the physical data environment - including data warehouses, systems, and applications -as well as the tools that support data collection, processing, storage, access, retrieval, and usage.

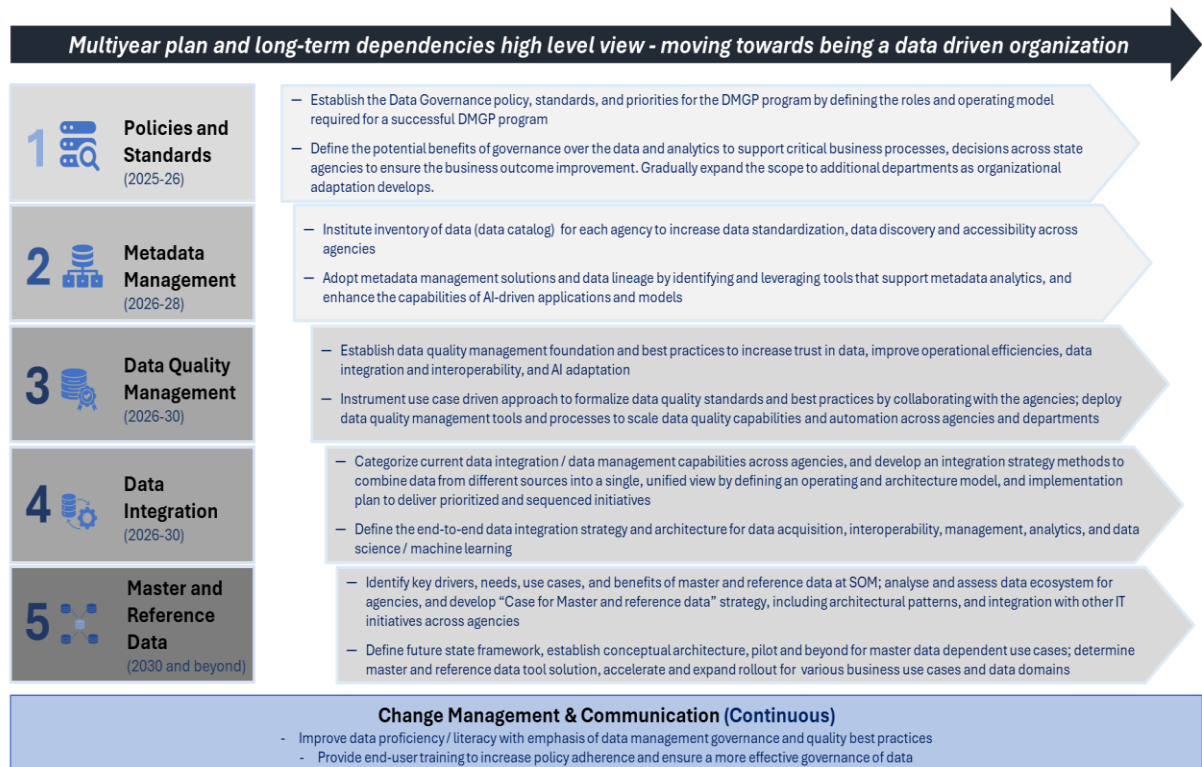
Data Custodians coordinate with MaineIT to ensure that technology systems and applications align with the overall data needs and standards of the business area or unit. All final IT Procurement decisions are made by MaineIT / Office of State Procurement. Data Custodians collaborate with Data Stewards and Data Officers to implement any changes needed for these systems and applications, and with Records Officers to ensure that data is correctly identified by record type for storage, archive, or destruction, as determined by retention schedules.

High-Level Activities and Responsibilities:

- Works jointly with business areas and DMGP to oversee data protection and the management of data assets.
- Implements and supports enterprise data governance policies, processes, and standards established by MaineIT and DMGP while ensuring compliance.
- Manages data by capturing, storing, retaining, and disposing of it in accordance with established requirements.
- Coordinates with Records Officers to ensure the implementation and management of data retention schedules while maintaining appropriate Disaster Recovery (DR) measures.
- Maintains data security by enforcing appropriate controls and protective measures to safeguard information.
- Collaborates with Data Officers and Data Stewards to define business requirements and use cases while supporting the development of data catalogs, data dictionaries, and data controls.
- Engages with Data Stewards and DMGP team to address concerns related to data quality, security, and privacy, facilitating resolution of data quality issues.
- Encourages uniformity in data management objectives, policies, procedures, tools, and methodologies.
- Provides input and feedback in the procurement of key technology platforms, including rules engines and data quality systems, while managing error handling workflows and data benchmarking processes.
- Consults with MaineIT to conduct impact analysis to assess changes to existing data sources, information architecture, security, and related elements.
- Identifies relevant data attributes and adopts systems of record (SOR) as authorized by MaineIT Enterprise Architecture and governance processes.
- Notifies and seeks approval from MaineIT Enterprise Architecture to ensure any changes to systems, processes, or data that impact data management are communicated to the DMGP, vendor (if applicable), relevant Data Stewards, and users.
- Performs root cause analysis for data-related issues and oversees data quality resolution across various data types.
- Monitors metrics and generates reports for designated data categories.

7.6 Organizational Change Management (OCM)

The DMGP Road Map is a 10-year vision for implementing enterprise data governance within the State of Maine. Although five distinct phases are identified, it is important to note that progress may not necessarily be linear, and work streams may occur in parallel across several phases, based on agency needs and readiness.



Central to this vision is Organizational Change Management (OCM). It is a shared responsibility among all layers of data governance and is crucial for the successful implementation of initiatives in each phase. Enterprise-level changes need to account for resistance, provide frequent and clear communication, and must articulate a clear shared vision of success. By integrating OCM with data governance programs, agencies can efficiently manage the human aspect of change, ensuring the effective and sustainable implementation of data governance practices through strategic communication and end-user training.

The DMGP, in collaboration with the Project Management Office (PMO) and agency Data Officers/Data Stewards, will identify opportunities for change management and ensure alignment with business, IT and established data management procedures. The DMGP and PMO will facilitate the communication of changes to data stakeholders. Some of the key activities addressed by OCM include:

- Coordinating the implementation of DMGP initiatives across agencies
- Ensuring effective and sustainable data governance practices through strategic communication
- Facilitating end-user training and workshops to enhance data literacy
- Managing changes that affect data access or protection as defined by applicable policies
- Efficiently managing process and system changes, reducing resistance to change, and achieving lasting transformation around the ways data is viewed as a strategic asset and catalyst for improved decision-making.

8.0 Related Policies and Documents

This Data Governance Policy functions in concert with the following policies:

- MRS [Title 5, Ch. 13 §282 \(3\)](#) - DAFS Commissioner responsibility to make data available for reporting to the Governor and Legislature
- MRS [Title 5, Ch. 163 §1982 \(9\)](#) - Agencies' responsibility and ownership of their respective data
- [PL 2021 C 717](#), An Act to Promote Equity in Policy Making by Enhancing the State's Ability to Collect, Analyze and Apply Data
- [PL 2023 C 581](#), An Act to Amend the State's Data Governance Program
- Relevant MaineIT and Information Security Policies (Information Security Policy, Data Exchange Policy, Data Classification Policy, Access Control Policy)

9.0 Policy Governance and Approval

Given the potential for changing conditions related to the Data Management and Governance Practice, this policy guidance must be flexible. Pursuant to PL 2023 C581, the DAFS Commissioner has identified the Chief Data Officer as their designee to amend this policy when the EDC deems it is appropriate to do so. All such modifications are reported to the DAFS Commissioner for review and approval by the next quarterly meeting.

On at least an annual basis, the DAFS Commissioner reviews, and where appropriate, updates this policy for submission to the EDC for review, feedback, and approval.

10.0 Review & Amendment

At least annually, this Data Governance Policy document is reviewed and updated as necessary by the Chief Data Officer. The changes adopted are to be placed into effect immediately upon approval by the DAFS Commissioner.

11.0 Data Governance Policy Document History

Owner: State Chief Data Officer

Recommending Party: State Chief Data Officer, Data Management and Governance Practice

Approver: Commissioner, Department of Administrative and Financial Services

Version Control:

Version	Date	Created By	Approved By	Next Review Date
1.0	01/09/2026	Paidipalli, Raja	Clark, Elaine	01/09/2027

12.0 Appendix / Glossary of Terms

Data Catalog - collection and classification of metadata

Data Governance – the Data Governance Institute describes data governance as “a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods.” Data governance is the ability to use demographic, socioeconomic, and spatial data to make better-informed policy decisions for programs and services

Data Inventory – types of data an organization currently collects, and what data it needs, but does not currently collect

Data Literacy - the ability to read, understand, create and communicate data in context, including an understanding of data sources and constructs, analytical methods and techniques applied, and the ability to describe the use case, application, and resulting value

Data Management - the processes, tools, and enabling technology that support Data Governance

Data Maturity – level of sophistication of an organization’s data management and governance policies, procedures, and practices. In the absence of written policies and procedures, it defaults to what is actually being done

Data Maturity Assessment – process by which organizations identify current practices and policies, data systems, data inventory, data catalog, and prohibitions and restrictions around legal or ethical sharing of data

Data Quality - the degree to which data is accurate, complete, timely, consistent with all requirements and business rules, and relevant for a given use

DMBOK – data Management International’s Data Management Body of Knowledge model. It contains 10 core domains:

- Data Quality
- Data Architecture
- Data Modeling and Design
- Data Storage and Operations
- Data Security
- Data Integration and Interoperability
- Document and Content Management
- Reference and Master Data
- Data Warehousing and Business Intelligence
- Metadata

Data Integration – unification of multiple data systems and technologies into one. Although some integration will occur, this will not be DAFS’s primary approach as there are currently over 1,200 disparate data systems, and centralizing all of this data into a single entity would likely create a security concern

Gap Analysis - comparison between the current state of an organization’s data management and governance policies and practices and its aspirational state

Interoperability - the ability of disparate data systems to work effectively together and share data. DAFS’s vision of Data Management and Governance Practice is to support interoperability among the State’s various data systems, rather than merging them into one (integration)

Metadata – “data about data.” This includes the purpose, date of creation, quality, location, author, file size and name. Much of this information can be de-identified to promote legal and ethical sharing of data.

Master and Reference Data – master and Reference data establish a single source of truth for critical business entities by minimizing data duplication and inconsistencies, streamlining operations, and enhancing data integration. This data is the backbone of all financial systems. When this information is inconsistent across different parts of an organization, essential business functions suffer.

Examples of master and reference data include budget units, merchant category codes, payroll information, office locations, and tax identification numbers.

Prohibitions and Restrictions - the laws, policies, and other safeguards or barriers that prevent an organization from sharing data

Structured Data – data that has a standardized format (usually a predefined data model) that makes it easier to access for reporting and other purposes

Unstructured Data - data that is not stored in a structured database format and does not follow a predefined data model. Examples include Microsoft Word documents, Excel spreadsheets, and PowerPoint presentations.