



**State of Oklahoma
Office of Management and Enterprise Services
Policies and Procedures**

Data Governance

Effective Date of Policy: 04/01/2019	Next Scheduled Review: 05/01/2020
Prior Policy:	Policy Number: OMES-029
Last Reviewed: 02/25/2019	Replaces Policy Number:
Date Policy Last Revised: 04/18/2018	
Approved: Dana Webb, as Designee of OMES Director John Budd	Approval Date: 02/25/2019

Reference

The Data Management Association International (DAMA) Data Management Body of Knowledge (DMBOK).

Policy

Data are state assets maintained to support Oklahoma’s efforts to meet its strategic goals and objectives.

To support these efforts, the Office of Management and Enterprise Services (OMES) data must be accessible, must correctly represent the information intended, and must be easily integrated across information systems. Therefore, this Data Governance Policy addresses the data governance structure and includes policy requirements on data access, data usage, and data integrity and integration.

The purpose of the OMES Data Governance Policy is to:

- Improve the privacy and security of the data, including confidentiality and protection from loss.
- Establish appropriate responsibility for the management of data as an organizational asset.
- Improve ease of access and ensure that once data are located, users have enough information about the data to interpret them correctly and consistently.

- Improve the quality of the data, resulting in greater accuracy, timeliness, and integrity of information for decision making.
- Ensure all data-related issues are resolved via the data governance structure adopted per this policy.

Procedure

This policy covers data governance for all of the agency's data assets (regardless of the system in which the data are stored) and data management knowledge areas, or functions, as defined by the Data Management Association's Guide to the Data Management Body of Knowledge (DAMA-DMBOK).

Anyone who creates, manages or uses OMES data is affected by this policy. Data governance executive sponsors, data owners, data stewards, and all other OMES employees who use data, regardless of the form of storage or presentation, should be familiar with this policy.

This Data Governance Policy shall be maintained by the manager of the Data Governance Program, approved by the OMES Data Governance Committee and the OMES division directors and published and communicated to all relevant parties. At a minimum, this policy shall be reviewed and/or updated annually.

Data Management Functions/Knowledge Areas

A policy shall be documented for each data management function/knowledge area represented in the diagram below. These policies must be referenced when reviewing or updating current data management procedures or when developing new data management procedures across the agency. At a minimum, each policy shall be reviewed and updated annually. The data management functions/knowledge areas include:

- Data Architecture
- Data Modeling and Design
- Data Storage and Operations
- Data Security
- Data Integration and Interoperability
- Documents and Content
- Reference and Master Data
- Data Warehousing and Business Intelligence
- Meta-data
- Data Quality

2013 Knowledge Areas



© DAMA International 2013

Data management procedures shall define the processes and procedures to be followed in order to meet the policy statements of the data management function policies.

Data and data management functions shall be measured, monitored and refined to ensure their effectiveness and quantify their value to the organization.

Data Governance Program and Framework

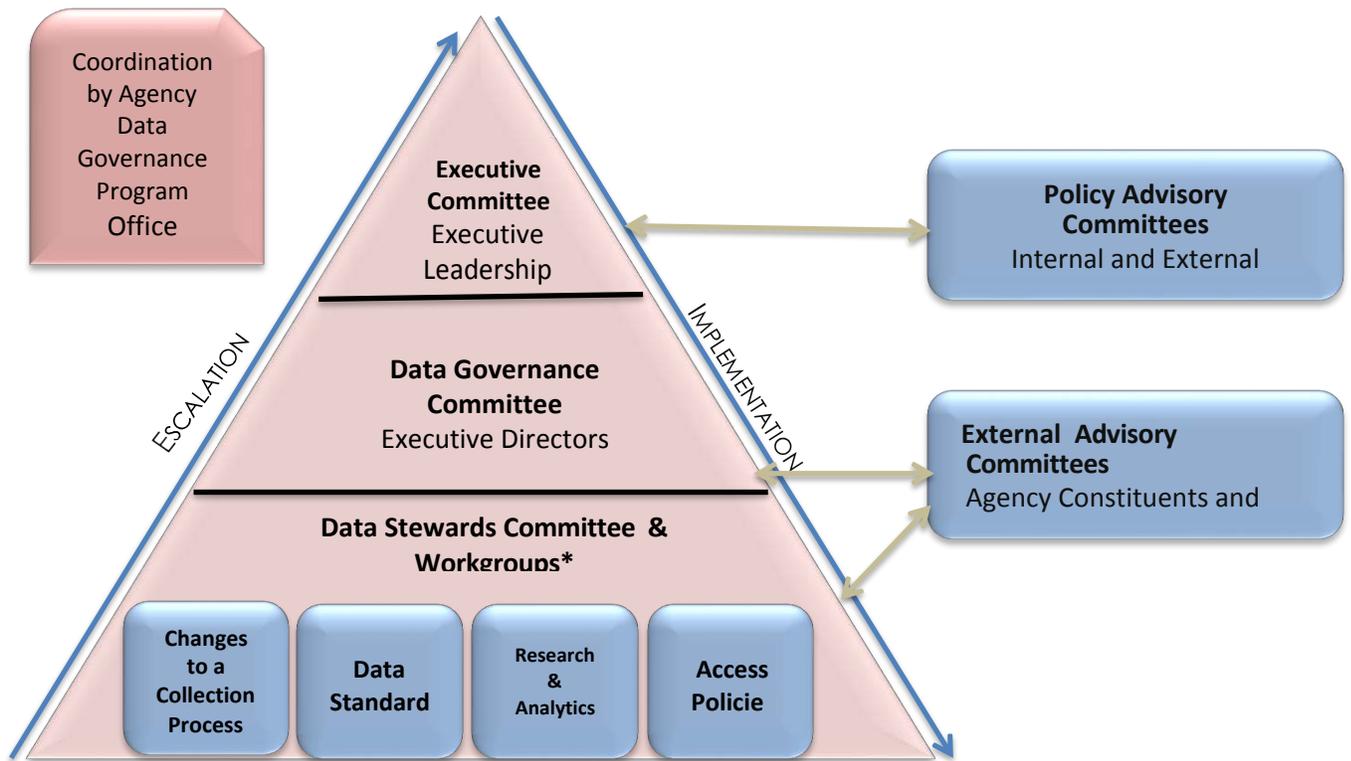
A Data Governance Program and framework shall be established, implemented, operated, monitored, reviewed, maintained and improved upon to ensure that appropriate authority and control (planning, guiding and monitoring) is applied to data, and that data are managed in line with legislative and other compliance obligations. The Data Governance Program shall be governed by the Data Governance Executive Committee, the Data Governance Committee, the Data Stewards Committee, and various data steward workgroups.

Data Governance Structure

Data Governance consists of the Data Governance Executive Committee, the Data Governance Committee, the Data Stewards Committee, and various data steward workgroups. Issues are identified and addressed by data stewards. Issues that cannot be resolved by data stewards are escalated up through the data governance structure to the Data Governance Committee and, if needed, the executive committee. The executive committee meets as needed. The Data

Governance Committee and Data Stewards Committee meet on a regular basis.

Data steward workgroups are created on an ad hoc basis at the request of individual data stewards.



*Examples of workgroups. Some may be engaged long-term and others short-term.

Data Governance Committees

Executive Committee – Responsible for supporting the Data Governance Program, identifying members to serve on the Data Governance Committee, and resolving issues escalated by the Data Governance Committee.

Data Governance Committee – Responsible for approving and enforcing data-related policies and standard procedures, resolving issues escalated by data stewards, and ensuring the overall quality of organizational data.

Data Stewards Committee and Data Steward Workgroups – Responsible for identifying data issues and possible solutions, and recommending and implementing data-related policies and initiatives.

Data Governance Roles

Executive Sponsor

An executive sponsor is a member of senior leadership who has planning and policy responsibility and accountability for major administrative data systems within their functional areas. By understanding the planning needs of the state, they are able to anticipate how data will be used to meet state and organizational needs.

Data Owners

Data owners are appointed by the executive committee. They are typically directors or managers who have authority to determine business definitions of data, grant access to data, and approve the secure usage of those data, for the functional areas within their delegations of authority. By understanding the information needs of the agency, data owners are able to anticipate how agency data can be used to strategically meet the agency's mission and goals.

Data Custodians

Data custodians are responsible for the operation and management of technology and systems that collect, store, process, manage, and provide access to agency data. Data custodians typically are associated with technical functions of the agency, but may also include systems administrators within all functional areas.

Data Stewards

Data stewards are responsible for implementing data policies. Additionally, data stewards have responsibility and authority for the day-to-day management of one or more types of agency data. Data stewards authorize and monitor the secure use of data within their functional areas to ensure appropriate access, accuracy, classification, privacy and security.

Data Users

Data users are authorized individuals who have been granted access to agency data in order to perform assigned duties or functions within the agency. When individuals become data users, they assume responsibility for the appropriate use, management and application of privacy and security standards for the data they are authorized to use. As such, data users must work with data stewards and data custodians to ensure that they understand any use of agency data beyond the initial scope requires approval by the appropriate data steward.

Data Governance Office (DGO)

The DGO facilitates and supports data governance and data stewardship activities, including:

- Keeping track of data stakeholders and stewards.
- Collecting and aligning policies, standards and guidelines from stakeholder groups.
- Arranging for the providing of information and analysis to IT projects as requested.
- Facilitating and coordinating data analysis and issue analysis projects.
- Facilitating and coordinating meetings of data stewards and data owners.
- Collecting metrics and success measures and reporting on them to data stakeholders.
- Providing ongoing stakeholder care in the form of communication, access to information, recordkeeping and education/support.
- Articulating the value of data governance and stewardship activities.
- Providing centralized communications for governance-led and data-related matters.
- Maintaining data governance records.