



DATA GOVERNANCE CHARTER



Contents

- 1. Introduction 3
- 2. Data Governance Framework..... 6
- 3. Data Governance Framework Components 7
 - Component # 1: Mission, Vision, and Value Statement.....7
 - Component # 2: Goals, Governance Metrics/Success Measures, Funding Strategies.....7
 - Component # 3: Data Rules and Definitions12
 - Component # 4: Decision Rights13
 - Component # 5: Accountabilities.....13
 - Component # 6: Controls16
 - Component # 7: Data Stakeholders17
 - Component # 8: Data Governance Organizational Structure / Data governance office.....17
 - Component # 9: Institutional Data stakeholders22
 - Component # 10: Data Governance Processes23
- Appendices..... 24

DRAFT

Figures and Tables

Figures

Figure 2 – SEI Capability Maturity Model8
Figure 2 – Data Governance Organizational Structure18

Tables

Table 1 – Decision Rights13
Table 2 – COBIT and ISO control elements16
Table 3 – Data Governance Office18

DRAFT

1. Introduction

This document describes the components of the proposed Data Governance Framework. Data Governance is the specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.

Data governance focuses on improving data quality, protecting access to data, establishing business definitions, maintaining metadata and documenting data policies. Effective data governance serves an important function within the University, setting the parameters for data management and usage, creating processes for resolving data issues and enabling data users to make decisions based on high-quality data and well-managed information assets. This is done by setting up a system of decision rights and accountabilities for data-related processes, executed according to agreed upon models.

This document also outlines the data governance framework that specifies the decision rights and governance structure, identifies roles, and specifies accountabilities for data stewardship and decision making. The framework aims to provide guidance to data stakeholders to manage institutional data, resolve issues and define processes for improving data quality.

DRAFT

SCOPE

At this initial stage, the scope of data governance is the management of structured institutional data, decisions regarding the collection, retention, duplication, quality control, definition and sharing of such data. Information governance, which will include records management and unstructured data is not within the scope of this data governance framework at the time of writing this document.

DRIVERS

The primary drivers for implementing data governance and this framework at the University of Calgary are as follows:

- improving data quality and thereby improving confidence in institutional data;
- facilitating and enabling auditable / certified reporting sources that will allow consumption of data from authoritative data assets that are certified for authenticity;
- identifying data ownership. Better accountability and data ownership will improve trust and confidence in data being reported both externally and internally;
- establishing agreed upon and enforceable Institutional agreements for data sharing and use;
- establishing consistency in understanding of data definition. Better understanding of data definitions will promote consistent usage;
- establishing right-sized data governance organization with cross-institutional representation that are accountable for decisions around management of data assets, structure, lifecycle, design and development standards and data flows;
- coordinating and controlling data library;
- developing well established data access management;
- establishing transparency of data usage;
- improving operating effectiveness and reducing administrative cost;
- establishing data error remediation process;
- producing effective data governance policies, standards, and procedures;
- enabling better quality information delivery and analytics;
- developing capability to respond to changes rapidly through impact analysis;
- improving quality, consistency and usability of master and reference data;
- establishing robust quality controls across the data life cycle;
- establishing accountability for data; and
- promoting business agility, better compliance and stronger insights.

PRINCIPLES

The following principles are set forth as minimum standards to govern the appropriate use and management of institutional data:

- institutional data is the property of the University of Calgary and shall be managed as a key asset;
- unnecessary duplication of institutional data is discouraged;
- quality standards for institutional data shall be defined and monitored;
- institutional data shall be protected;
- institutional data shall be accessible according to defined needs and roles;
- institutional metadata shall be recorded, managed and utilized;
- institutional representatives will be held accountable to their roles and responsibilities;
- necessary maintenance of institutional data shall be defined;

- resolution of issues related to institutional data shall follow consistent processes; and
- data stewards are responsible for the subset of data in their charge.

DRAFT

2. Data Governance Framework

The data governance framework proposed in this document is adapted from the Seiner Non-invasive data governance framework, DGI data governance framework, and certain principles from the DAMA data governance framework. The goals of this framework are to formalize accountability, roles and responsibilities by applying them to existing structure and processes. This will ensure transparency and collaboration in improving production, definition and usage of data.

DRAFT

3. Data Governance Framework Components

COMPONENT # 1: MISSION, VISION, AND VALUE STATEMENT

MISSION

- To undertake a leadership role in the creation, implementation and oversight of the enterprise-wide information and data management goals, standards, practices and processes aligned with the goals of the institution.
- To provide expert advice and support in relation to all aspects of information and data governance including data ownership, data protection, data privacy, and information usage, classification and retention.
- To promote data governance at an executive and senior management level.
- To build a data governance framework that establishes consistent definition and understanding of data, establishes ownership of data, establishes how metadata is managed, and establishes organizational roles and responsibilities.

VISION

Enable the University community to treat information as an institutional asset that can be used and shared with confidence to support evidence based decision making and take informed action.

VALUE STATEMENT

The data governance program will create data definitions, influence data strategy, and build an overarching data governance model to increase confidence in and usability of institutional data.

COMPONENT # 2: GOALS, GOVERNANCE METRICS/SUCCESS MEASURES, FUNDING STRATEGIES

GOALS

- Establish a data governance advisory group (DGAG) with representation from across the university and develop group terms of reference
- In collaboration with Institutional Asset Management Committee (IAMC), finalize membership of DGAG (not to exceed 10 members)
- Engage the DGAG as part of the RFP development for the data governance tool.
- Develop and issue an RFP for a data governance tool, with the engagement of the DGAG.
- Develop a data governance framework and fine tune it in collaboration with the DGAG to address the following:
 - rules of engagement regarding governance metrics and success measures, funding strategies, data rules and definitions, decision rights, accountabilities, and controls;
 - structure and definition of people and organizational bodies;
 - proactive, reactive, and ongoing data governance processes; and
 - data sharing requirements and rules.

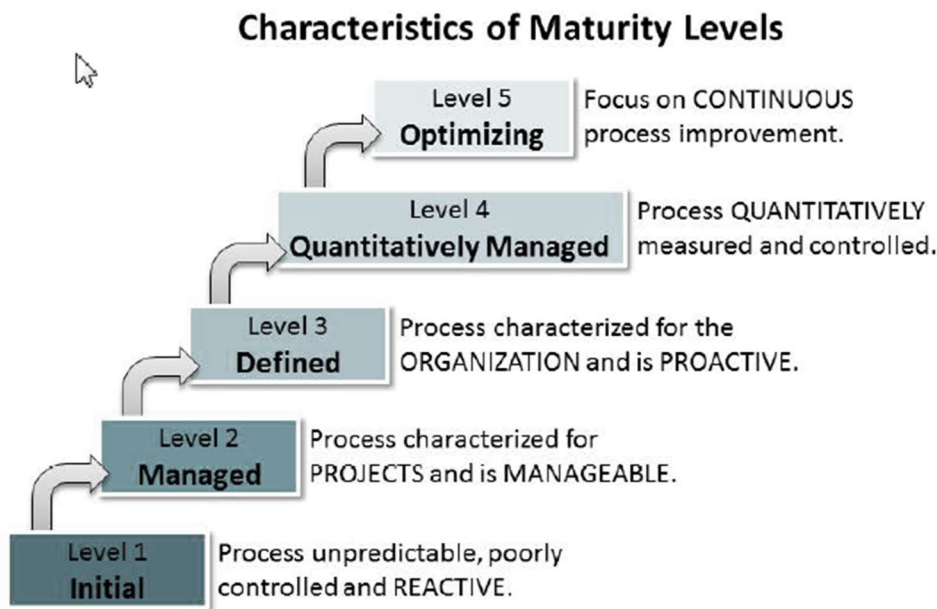
GOVERNANCE METRICS / SUCCESS MEASURES

We propose using the Data governance maturity model from Stanford as a baseline to develop the University of Calgary model . (Reference: [Data Governance Maturity Model from Stanford](#))

Concept of the Process Maturity Levels

Developed by the Software Engineering Institute (SEI) in 1984, the Capability Maturity Model (CMM) is a methodology used to develop and refine an organization's software development process and it can be easily applied to an organization's DG program and processes. The CMM describes a five-level graduated path that provides a framework for prioritizing actions, a starting point, a common language and a method to measure progress. Ultimately, this structured collection of elements offers a steady, measurable progression to the final desired state of fully mature processes (IBM, 2007).

Figure 1 – SEI Capability Maturity Model



- Level 1: processes are ad hoc, and the environment is not stable. Success reflects the competence of individuals within the organization, rather than the use of proven processes.
- Level 2: successes are repeatable, but the processes may not repeat for all the projects in the organization.
- Level 3: the organization's set of standard processes are used to establish consistency across the organization.
- Level 4: organizations set quantitative quality goals for both process and maintenance.
- Level 5: quantitative process-improvement objectives for the organization are firmly established and continually revised to reflect changing business objectives, and used as criteria in managing process improvement.

THE COMPONENT-DIMENSIONS

The proposed Maturity Measurement tool from Stanford University, focuses both on foundational and project aspects of Data Governance (DG). It has two types of components and three Dimensions:

COMPONENTS

1. The foundational components (Awareness, Formalization and Metadata) of the maturity model focus on measuring core DG competencies and development of critical program resources.
 - Awareness: The extent to which individuals within the organization have knowledge of the roles, rules, and technologies associated with the data governance program.
 - Formalization: The extent to which roles are structured in an organization and the activities of the employees are governed by rules and procedures.
 - Metadata: Data that 1) describes other data and IT assets (such as databases, tables and applications) by relating essential business and technical information and 2) facilitates the consistent understanding of the characteristics and usage of data. Technical metadata describes data elements and other IT assets as well as their use, representation, context and interrelations. Business metadata answers who, what, where, when, why and how for users of the data and other IT assets.
2. The project components (Stewardship, Data Quality and Master Data) measure how effectively DG concepts are applied in the course of funded projects (Stanford, 2011). The project components (Stewardship, Data Quality and Master Data) measure how effectively DG concepts are applied in the course of funded projects (Stanford, 2011).
 - Stewardship: The formalization of accountability for the definition, usage, and quality standards of specific data assets within a defined organizational scope.
 - Data Quality: The continuous process for defining the parameters for specifying acceptable levels of data quality to meet business needs, and for ensuring that data quality meets these levels. (DMBOK, DAMA)
 - Master Data: Business-critical data that is highly shared across the organization. Master data are often codified data, data describing the structure of the organization or key data entities (such as “employee”).

DIMENSIONS

Three dimensions (People, Policies and Capabilities) further subdivide each of the six maturity components, focusing on specific aspects of component maturation.

1. People: Roles and organization structures.
2. Policies: Development, auditing and enforcement of data policies, standards and best practices.
3. Capabilities: Enabling technologies and techniques.

PROPOSED METRICS TO MEASURE SUCCESS OF DATA GOVERNANCE PROGRAM

Metrics are important to establish a baseline and know where the DG program is going and progressing. It will help us align expectations, create a starting point and define and measure success. In addition, metrics helps to communicate the value of the data governance program to the stakeholders. It is important to note that metrics will need to change and morph based on the focus of the program.

Each metric needs to be clearly defined, capable of measurement, and directly relevant to improving program effectiveness. The Data Governance Advisory Group will be a good judge, and they should review and approve all metrics. Metrics are created by either DGAG or Communities of Practice (COP) and approved by DGAG and IAMC. As the primary focus of this phase of Data governance is encouraging adoption of the program to build consensus on data definition and data sharing agreements, the following progress metrics category will be important.

People Metrics

Metrics in this category relate to tasks and activities that go into aligning, assigning and onboarding people as part of the program as well as the number of people who have been trained, and their ongoing participation. Other ways that this area can be measured is by tracking:

- number of resolved issues;
- the number of data owners identified;
- the number of projects approved; and
- program adoption rate by departments and university staff.

Processes Metrics

Adoption of the data governance policies and practices is a great way to measure how well users understand them.

Technology Metrics

Measurement in this category could look at:

- integrity of the data across systems, reports etc.;
- the number of data targets using master data;
- the quantity of lineage documented; and
- the adoption and usage of the data governance tool.

Data Metrics

In this category the measurement will be related to data quality. Instead of looking at all the data at the institutional, the focus initially should be on certain sets of high impact, high usage data elements. Some of the proposed metrics for the first phase of the data governance program are number of data:

- quality issues resolved by communities of practice;
- quality issues escalated to DGAG and resolved;
- quality issues escalated to IAMC and resolved;
- access issues resolved by communities of practice;
- access issues escalated to DGAG and resolved;
- access issues escalated to IAMC and resolved; and
- owners identified and confirmed.

FUNDING STRATEGIES

Implementation of the data governance tool will require an initial investment of approximately \$200,000 to purchase the data governance tool and the implementation service. Ongoing funding will be required to continue the sustainment of the tool and 1-2 Full-time Equivalent (FTE) (Management and Professional Staff (MaPS) (P2 or P3) to coordinate the data governance program implementation and operation of the tool.

DRAFT

COMPONENT # 3: DATA RULES AND DEFINITIONS

DATA RULES AND DEFINITIONS

Data usage, discovery and sharing is improved when users have access to data definitions that define attributes of the data elements as well as Data rules that describe the usage of the data. ISO 11179 is a global standard to provide guidelines for standardizing and registering data elements. It consists of:

- Specification and Standardization of Data Elements;
- Classification of Data Elements;
- Basic Attributes of Data Elements;
- Rules for Data Definitions Naming; and
- Identification of Data Elements Registering and Storing Data Elements.

In order to have consistent understanding of data, a data dictionary needs to be developed to produce and record data definitions. When data is both understandable and highly comparable there is more potential for data integration. Consistent use of common data dictionary elements would help to increase data transparency for data developers and users. A simple data dictionary is an organized collection of data element names and definitions, arranged in a table. It may describe all the data holdings of an organization, a part of the holdings or a single database. The following list contains possible contents of a data dictionary:

- Data Element Domain: The context within which the data element exists (e.g. Student, Finance, HR, Accounts etc.);
- Data Element Number: A unique number for the data element used in technical documents;
- Data Element Name: Commonly agreed, unique data element name;
- Data Element Field Name(s): Names used for this data element in applications, reports and database schemas;
- Data Element Definition: Description of the meaning of the data element;
- Data Element Unit of Measure: Scientific or other unit of measure that applies to the data value;
- Data Element Value: The reported value;
- Data Element Precision: The level to which the data element value will be reported (e.g. miles to 2 decimal places);
- Data Element Data Type: Data type (characters, numeric, etc.), size and, if needed, any special representation that applies to the data element;
- Data Element Size: The maximum field length as measured in characters and the number of decimal places that must be maintained in the database;
- Data Element Field Constraints: Data Element is a required field (Y/N); Conditional field (c); or a null field: Required fields (Y) must be populated. Conditional fields (C) must also be populated when another related field is populated (e.g. if a city name is required a postal Code may also be required). “Not null” also describes fields that must contain data. “Null” means the data type is undefined (note: a null value is not the same as a blank or zero value);
- Data Element Default Value: A value that is predetermined -it may be fixed or a variable, like current date and time of the day; and
- Data Element Edit Mask: An example of the actual data layout required (e.g. yyyy/mm/dd).

COMPONENT # 4: DECISION RIGHTS

DECISION RIGHTS

Decision rights establishes who is responsible for making what type of decisions. Table 1 list some of the decision rights around data definition, retention, naming etc. More can be added to this list.

Table 1 – Decision Rights

	IAMC/ Trustees	DGAG	Stewards	Community of practice	Decision Style	Delegation
Confirm Data definition						
Define Data retention						
Develop Data definition						
Enforce data retention						
Data naming						
Data sharing policy						
Data sharing audit						
Decision on student definitions						
Define Data Producing processes						
Create business data dictionary						
Plan data quality initiatives						

COMPONENT # 5: ACCOUNTABILITIES

Several roles and responsibilities govern the management of, access to and accountability for institutional data. These roles and their accountabilities are listed below:

Data trustees

Data trustees are defined as institutional officers (e.g., vice presidents, vice provosts, deans and chancellors) who have authority over policies and procedures regarding business definitions of data and the access and usage of that data within their delegations of authority. Data trustee appoint data stewards for specific subject area domains.

As a group, the data trustees are responsible for:

- Actively participating in the Information Asset Management Committee.
- Approving data management policies, guidelines, standards and procedures developed by the Data Governance Advisory Group
- Approving changes to the scope of functional areas.

	<ul style="list-style-type: none"> Resolving issues of procedure escalated by the Data Governance Advisory Group
<p>Data stewards</p>	<p>Data stewards are university business unit officials who have direct operational-level responsibility for the management of one or more types of institutional data and have the authority to make decisions. They are responsible for promoting appropriate data use through planning, policy, and protocols at the institution.</p> <p>As a group, the data stewards are responsible for:</p> <ul style="list-style-type: none"> Actively participating in the Data Governance Advisory Group. Reviewing quality metrics and assessment of progress toward improvements in data integrity. Prioritizing data issues for resolution. Defining the scope of business data domains and approving changes. Coordinating data definitions and resolving stewardship issues for data elements that span multiple functional areas and/or units. As individuals, the data stewards also have specific responsibilities and authority for the management, access, use, definition and quality of data that pertains to their functional areas and/or is deemed to be under their purview. These responsibilities include: <ul style="list-style-type: none"> Appointing data custodians and delegate operational stewardship accountabilities. Establishing and managing working groups (Communities of practice) that define data and resolve data quality issues. Reviewing and approving data definitions, compliance and access classifications (i.e. UClass). Proposing, reviewing and approving new business terms. Approving the use of data by business units and/or research Approving and ensuring compliance regarding the release of, responsible use of and access to business unit data.
<p>Data custodians</p>	<p>Data custodians are system administrators responsible for the operation and management of systems and servers that collect, manage and provide access to institutional data. Individuals in business units responsible for ensuring that policies are followed within a specific area and that local processes are consistent with university policies and procedures. Both as individuals and collectively as part of a business domain working group, data custodians 'responsibilities include:</p>

	<ul style="list-style-type: none"> • Developing data definitions. • Assessing and documenting data compliance classifications. • Classifying data into access categories. • Reviewing and approving requests for data access. • Assessing data quality. • Identifying and documenting data issues and ensuring the issues are addressed. • Identifying source systems of record.
Data users	<p>Data users are university units or individual university community members who have been granted access to institutional data in order to perform assigned duties or in fulfillment of assigned roles or functions within the university; this access is granted solely for the conduct of university business.</p> <p>Data users are responsible for:</p> <ul style="list-style-type: none"> • Complying with the institutional data policies outlined in university data usage policies • Understanding the definition, quality and usage limitations of data. • Safeguarding their data access privileges.

DRAFT

COMPONENT # 6: CONTROLS

Data Governance controls are necessary elements in ensuring data is managed in a manner that creates consistency, enforces value, and maintains security. All Data Governance frameworks require a firm grounding in reasonable controls.

Implementing controls in an institution as diverse as the University of Calgary is wrought with challenges from a perspective and complexity outlook. Luckily however from both a Control Objective for Information and Related Technologies (COBIT) and International Organization for Standardization (ISO) perspective¹, the University of Calgary has already developed a firm foundation of controls in its use of institutional policies and procedures.

ISO control elements are built of the following elements:

- Security policies;
- Organization of information security;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and Operations Management;
- Access control;
- Information systems acquisition;
- Development and maintenance;
- Info. security incident management;
- Business continuity management; and
- Compliance.

Using these two different standards, and through analysis of various artifacts at the University of Calgary, it is clear that the University has already touched upon these areas of topic to a variety of scopes and depth (Table 2).

Table 2 – COBIT (Control Objective for Information and Related Technologies) and ISO (International Organization for Standardization) control elements

U of C ARTIFACT Name of artifact	COBIT ALIGNMENT Elements artifact aligns with COBIT	ISO ALIGNMENT Elements artifact aligns with ISO
Information Security Classification Standard ²	U of C artifacts holistically meet the requirements of the COBIT control elements definition.	Security Policy, Access Control
Information Asset Management Policy ³		Security Policy, Asset Management, Physical and Environmental Security, Business Continuity Management, Organization of Information Security, Communications & Operations Management
Acceptable Use of Information Assets Policy ⁴		Compliance, Human Resources Security

¹ Both COBIT and ISO are industry thought leaders regarding Information Technologies and all its elements, including Data Governance. From a CO

² http://www.ucalgary.ca/policies/files/policies/im010-03-security-standard_0.pdf

³ <http://www.ucalgary.ca/policies/files/policies/information-asset-management-policy.pdf>

⁴ <http://www.ucalgary.ca/policies/files/policies/Acceptable%20Use%20of%20Information%20Assets%20Policy.pdf>

COMPONENT # 7: DATA STAKEHOLDERS

To be identified in Phase 2 of the Data Governance initiative. The list shall be maintained on a central repository/site accessible to everyone at the University.

COMPONENT # 8: DATA GOVERNANCE ORGANIZATIONAL STRUCTURE / DATA GOVERNANCE OFFICE

No one person, department, division, school or group "owns" data, even though specific units bear some responsibility for certain data. The "data ownership" in this framework refers to the stewardship of institutional data by business units. Several roles and responsibilities govern the management of, access to and accountability for institutional data. These roles and their accountabilities are shown in

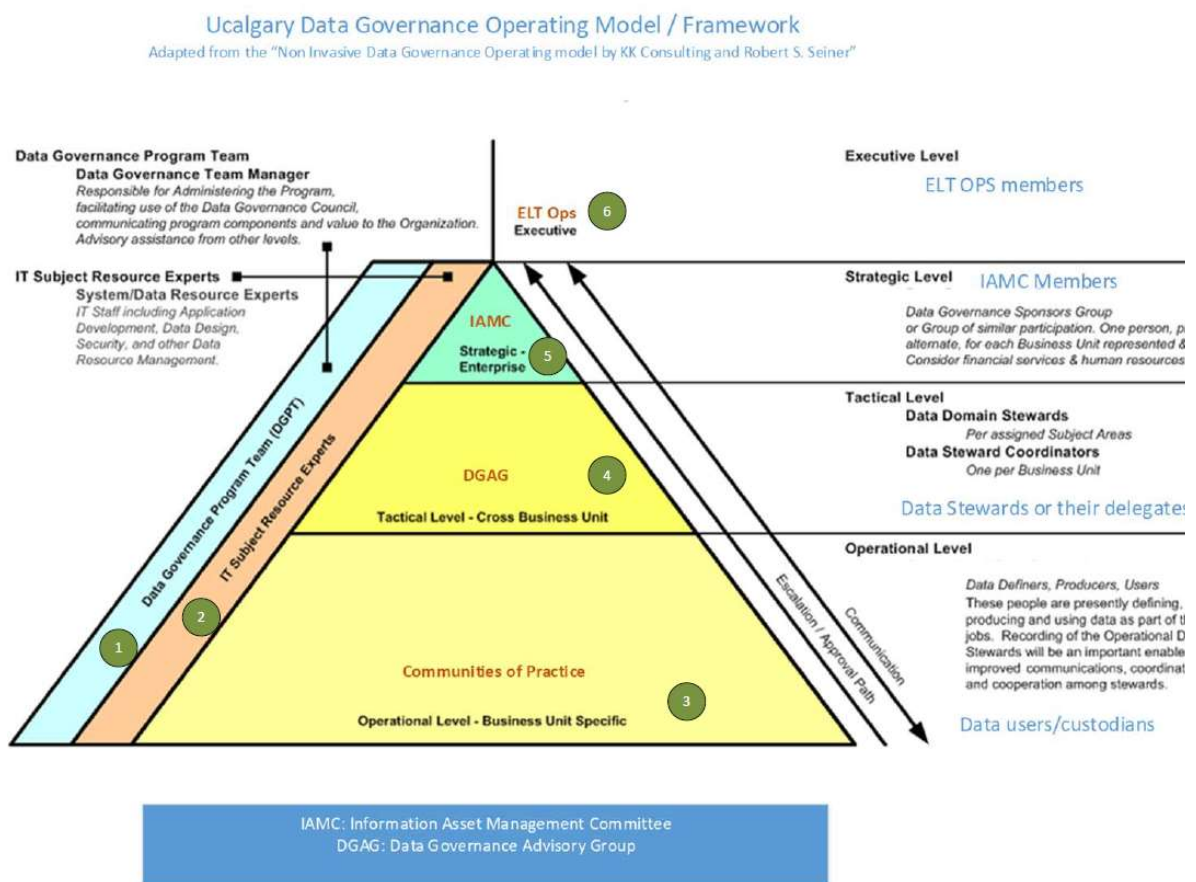


Figure 2 – Data Governance Organizational Structure

Table 3.

Ucalgary Data Governance Operating Model / Framework

Adapted from the "Non Invasive Data Governance Operating model by KK Consulting and Robert S. Seiner"

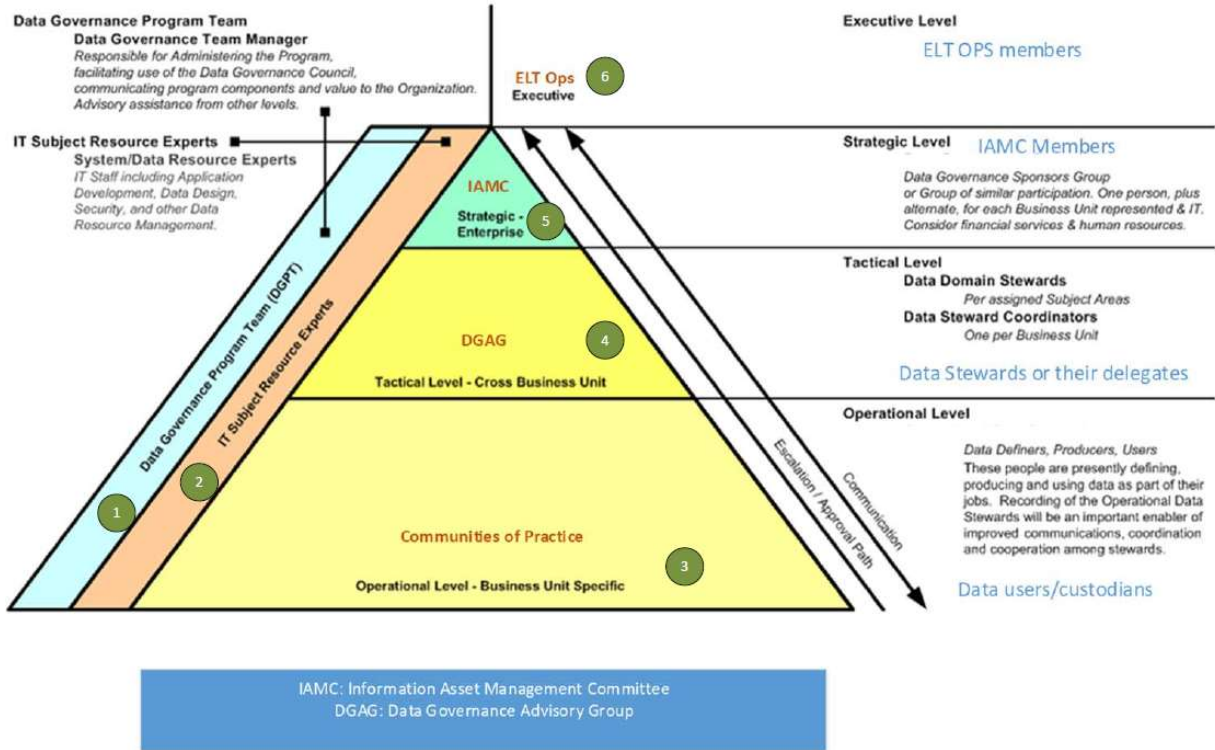


Figure 2 – Data Governance Organizational Structure

Table 3 – Roles in Data Governance

Role	Accountability
1. Data governance program team (DGPT)	<p>This group is comprised of select cross functional data custodians, stewards, the data governance administrator(s) and IT SMEs responsible for:</p> <ul style="list-style-type: none"> ▪ Architecting the solution and framework; ▪ Administering data governance, including facilitating data governance advisory group meetings; ▪ Providing the agenda items for the data governance advisory group and information asset management meetings to the approved and discussed; ▪ Facilitating data governance organization, tactical and operational stewards, DGAG and IAMC involvement; ▪ Developing and delivering data governance educational, awareness and mentoring materials;

	<ul style="list-style-type: none"> ▪ Providing quality assurance – oversight, monitor, and report results to governance council; ▪ Establishing, maintaining, and periodically reviewing and recommending changes to data governance policies, standards, guidelines, and procedures; ▪ Assisting in defining data quality metrics for periodic release ▪ Supporting data quality issue analysis and remediation for “strategic” data; and ▪ Conducting audits to ensure that policies, procedures and metrics are in place for maintaining/improving the program.
<p>2. IT Subject Resource Expert (Data SME and System SME)</p>	<p>Primarily composed of staff from IT System administration, PMO, IT Governance</p> <ul style="list-style-type: none"> ▪ Focusing on consistent protection/classification of data by data classification (confidential, public, internal use, ...); ▪ Technical handling of data to meet data classification requirements; ▪ Securing IT infrastructure on behalf of the business units that own or have responsibility for data; ▪ Assuring that sensitive data, regardless of format, is protected at all times by only using approved equipment, networks, and other controls; ▪ Championing the integration of data governance within the standard project methodology; ▪ Ensuring that standard project methodology is followed and that policies, procedures and metrics are in place for maintaining/improving data quality and the creation, capture and maintenance of metadata; ▪ Ensuring that all “strategic” data is modeled, named, and defined consistently; ▪ Ensuring that projects source and utilize data as much as is feasible from the designated system of record; ▪ Providing technical support for ensuring data quality; ▪ Providing technical support for data governance and data cleansing efforts where required; and ▪ Ensuring that metadata critical to data governance is included in the metadata resource and is accessible.
<p>3. Working groups / Communities of practice</p>	<p>Communities of practice (CoP) are composed of business representatives and serve as the data authority for their business area. Responsibilities include:</p> <ul style="list-style-type: none"> ▪ Ensuring data quality through fit-for-purpose requirements which are developed by the data owners; ▪ Identifying and prioritizing improvement of key systems or processes; ▪ Supporting the university’s data quality efforts through accountability to, and close interaction with, Data Governance Advisory group; ▪ Recommending projects based on their usage of the data within their areas of the organization; ▪ Defining the data that will be used by the organization, how that data will be used, and how that data will be managed; ▪ Producing, creating, updating, deleting, retiring, archiving the data that will be managed; ▪ Creating/reviewing/approving data definitions; ▪ Integrity and quality of data definition; ▪ Producing, creating, updating, deleting, retiring, and archiving the data that will be managed; ▪ Integrity and quality of the data created or updated in their department or process; ▪ Identifying and classifying data access levels; ▪ Identifying and documenting regulatory and legal/risk issues including data retention requirements;

	<ul style="list-style-type: none"> ▪ Supporting/sharing knowledge w/other stewards; ▪ Communicating new and changed business requirements to individuals who may be impacted; and ▪ Communicating concerns, issues and problems with data to the individuals that can influence change and the DGAG.
<p>4. Data governance advisory group</p>	<p>This working group is comprised of cross functional data stewards or their designate from all data trustee portfolios. When acting in role of data domain steward, affiliation to business unit becomes secondary. Responsibilities include:</p> <ul style="list-style-type: none"> ▪ Championing a data-centric culture across the university; ▪ Promoting and enforcing the best practices of the Data Governance Organization; ▪ Approving new data governance initiatives and projects; ▪ Maintaining alignment with institutional strategy; ▪ Helping resolve critical data governance issues; ▪ Providing conflict resolution; ▪ Championing the Data Governance Organization; ▪ Promoting acceptance of the data governance best practices, standards and guidance; ▪ Enabling and empowering the data users, custodians and communities of practice(s); <p>Facilitating and supporting data governance and data stewardship activities, including:</p> <ul style="list-style-type: none"> ▪ keeping track of data stakeholders and stewards; ▪ providing liaisons to other disciplines and programs, such as data quality, compliance, privacy, security, architecture and IT governance; ▪ collecting and aligning policies, standards and guidelines from these stakeholder groups; ▪ arranging for the providing of information and analysis to IT projects as requested; ▪ facilitating and coordinating meetings of data stewards; ▪ collecting metrics and success measures and reporting on them to data stakeholders and university leadership; ▪ providing ongoing stakeholder care in the form of communication, access to information, record keeping and education/support; ▪ providing centralized communications for governance-led and data-related matters; ▪ maintaining governance decision records; ▪ Involved/facilitator in cross business unit resolution of data definition, production and usage issues; ▪ Escalating well-documented issues to the strategic level (IAMC) with or without recommendation; ▪ Documenting data classification rules, compliance rules, business rules for data in their domain (may delegate this); ▪ Making certain the rules are communicated to all stakeholders of data in that domain (may delegate); and ▪ Participating in tactical groups for finite periods of time to address specific issues and projects related to their domain and business unit and subject area.
<p>5. Information Asset Management Committee</p>	<p>The committee chaired by the General Counsel is responsible for overseeing the management and protection of information assets. Responsibilities include:</p> <ul style="list-style-type: none"> ▪ Approving data policy, data role framework, methods, priorities, tools, etc.; ▪ Pushing data governance into their areas by actively promoting improved data governance practices; ▪ Making decisions at a strategic level in a timely manner given the appropriate knowledge to make that decision;

	<ul style="list-style-type: none"> ▪ Meeting regularly (or send alternate), read minutes to stay informed of data governance program activities; ▪ Identifying and approving of pivotal data governance roles including cross-enterprise domain stewards and coordinators; and ▪ Advising the data governance council owner in applying data governance to risk management, compliance, business unit-specific governance interests.
5. ELT members	All ELT members are data trustees and are responsible for sponsoring, approving, championing the enterprise strategic plan and policy; Communicating expectations and requirements for data governance; and Identifying and prioritizing data quality initiatives.

DRAFT

COMPONENT # 9: INSTITUTIONAL DATA STAKEHOLDERS

DATA TRUSTEES

Trustees are ELT Member who has decisionmaking authority with respect to Business Information Assets for their functional area or department.

DATA STEWARDS

Data stewards are university business unit officials who have direct operational-level responsibility for the management of one or more types of institutional data and have the authority to make decisions. Data stewards will be identified by the data trustees for specific data domains. They are responsible for promoting appropriate data use through planning, policy, and protocols at the institution. A list of identified data stewards will be maintained on a central repository/site accessible to everyone at the University.

DATA CUSTODIANS

Data custodians are system administrators responsible for the operation and management of systems and servers that collect, manage and provide access to institutional data.

DATA USERS

Data users are university units or individual university community members who have been granted access to institutional data in order to perform assigned duties or in fulfillment of assigned roles or functions within the university.

COMPONENT # 10: DATA GOVERNANCE PROCESSES

An important key to successfully maintaining data governance comes in the form of consistent and well thought out processes. The Data Governance Institute (DGI) distinguishes at a high level three distinct categories of required data governance processes:

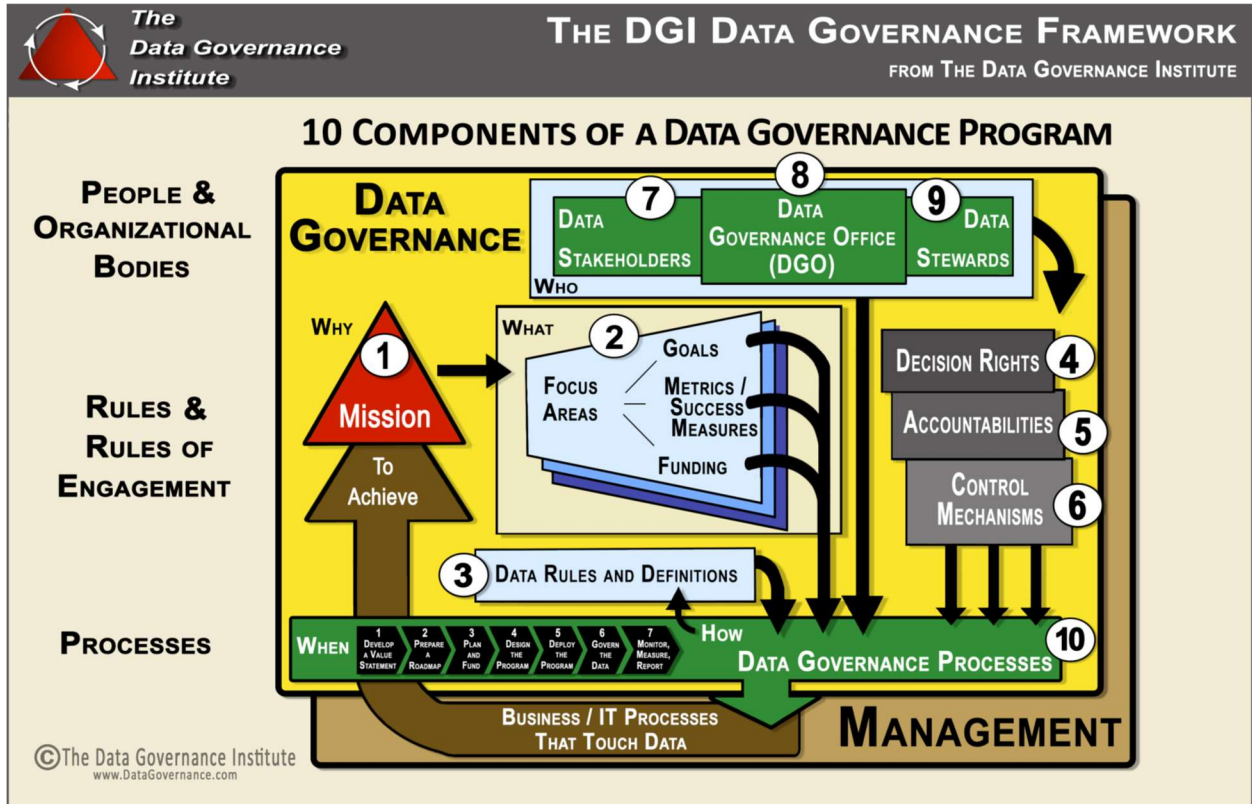
- Proactive: Processes pertaining to successfully setting up and evolving the data governance framework
- Ongoing: Processes pertaining to successfully maintain the data governance framework.
- Reactive: Processes pertaining to addressing ad hoc items that come about when utilizing the data governance framework.

DRAFT

Appendices

DOCUMENT HISTORY

S.No	Description of Change	Version No.	Date	Prepared by	Approved by
1.0	Initial Version	1.0	March 29 th , 2018	Data Governance Program Core Team (Nathan Hunt, John Gretton, Jeff Bowes, Adnan Ahmed, Kim Longmuir, Sandeep Banerjee)	
2.0	Changed component 5,8,9 to incorporate the non invasive data governance framework components. Removed Component # 5: Accountabilities	2.0	April 20,2018	Adnan Ahmed	
3.0	Changed Component # 10 Updated "Drivers" under the "Introduction" section	3.0	April 24 th , 2018	Nathan Hunt / Sandeep Banerjee	
4.0	Spell-check	4.0	April 29, 2020	Jean Gomes, OIA	



Appendix B: Sample questionnaire

Sample Questionnaire for Maturity Assessment

Metadata	People		Policies		Capabilities			
	Qualitative	Quantitative	Qualitative	Quantitative	Qualitative	Quantitative		
	1	No defined roles related to DG.		1	No formal DG policies		1	Classes of DG capabilities are not defined.
2	DG roles and responsibilities have been defined and vetted with program sponsors.		2	High-level DG meta-policies are defined and distributed.	Meta-policies defined, documented and approved.	2	Classes of DG capabilities are defined and homegrown technical solutions are used within some organizational functions.	DG capabilities with solutions by functional area. Reuse of technical solutions by functional area.
3	Some roles are filled to support DG needs and participants clearly understand responsibilities associated with their roles.	Participants in approved roles.	3	Data policies around the governance of specific data are defined and distributed as best practices.	Best practices/standards/policies identified, documented and approved.	3	Homegrown technical solutions are adopted as best practices for some classes of capabilities and made available throughout the institution.	Capabilities approved as organization recommended solutions.
4	DG roles are organized into reusable schemas which are designed to support specific data and functional characteristics. There is broad (but inconsistent) participation in DG.	Program areas in compliance with defined schemas. Percent of roles filled.	4	Data policies become official organization data policies and compliance with approved data policies is audited.	Official data policies approved. Audits are done to ensure compliance.	4	All defined classes of DG capabilities have an available solution.	Usage of standard solutions by project. Uses of non-standard solutions by project.
5	DG organizational schemas are filled as defined, meet regularly and document activities.	Staff from each defined schema meets to plan. Minutes produced.	5	Compliance with official organization data policies is actively enforced by a governing body.	Number of exceptions to official data policies (lower is better).	5	All defined classes of DG capabilities are mandatory for assigned systems or critical data.	Usage of non-standard solutions by project (lower is better). No use of solution by project.

DRAFT

DRAFT