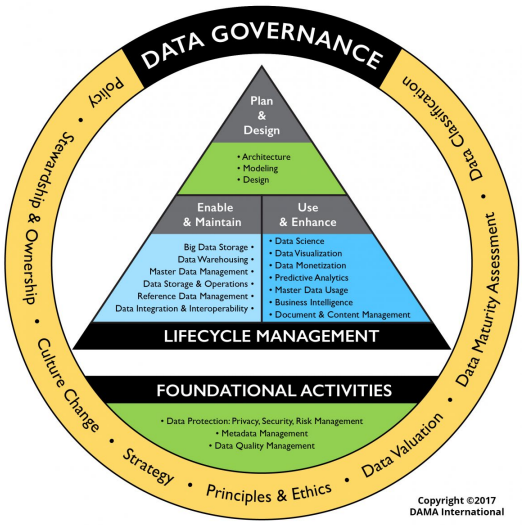
Data Governance By-Laws, Policies, Standards and Coordinating Bodies for Wichita State University Data Systems and Reporting Standards



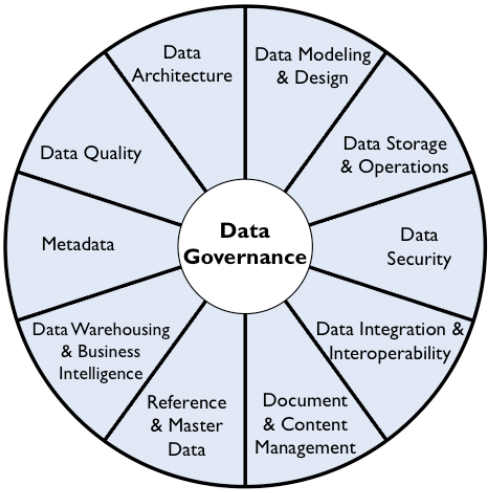


Table of Contents

1. Mission & Principles
   - 1.1 Mission
   - 1.2 Data Governance Principles

2. Data Governance Structures
   - 2.1 Data Trustee (DT) Level
   - 2.2 Data Management Committee (DMC) Level
   - 2.3 Data Custodians (DC) Level

3. Roles
   - 3.1 Data Governance Database Roles

4. C-Suite Related Roles and Coordinating Bodies
   - 4.1 C-Suite Compliance Officers
   - 4.2 Coordinating Development and Advisory Bodies

5. Data Access and Transfer Authorization
   - 5.1 Data Owner Role in Data Access
   - 5.2 Submitting Data Request
   - 5.3 Qualtrics and Survey Data
   - 5.4 Third-Party Vendor Data Transfers
   - 5.5 Vendor Out-Bound Data Inventory

6. Role of Data Governance: “Who is in Charge & Why”

7. Data Management Activities Overseen by Data Governance Policies

Appendix

Data Governance By-Laws, Policies, Standards and Coordinating Bodies for Wichita State University Data Systems[1] and Reporting Standards

1. Mission & Principles

1.1 Mission

Several data systems[1] exist which the university community can use to inform decision-making, planning and reporting. The mission of the Data Governance Council (DGC) is to provide oversight to these data systems to ensure data integrity, best practices in data management, reporting standards, information consistency, and security access. In addition, the Data Governance Council is charged (see Appendix A for official charge) with identifying data and reporting needs related to strategic planning priorities and the sharing of business knowledge across divisions to ensure data and reporting optimization related to the latest business practices within units. The Data Governance Council provides compliance with the Higher Learning Commission (HLC) requirements related to institutional data used for accreditation.

1.2 Data Governance Principles

1.2.1 Data must be recognized as a valued and strategic enterprise asset that must be managed effectively.

Accurate, timely data are the critical foundation for effective decision-making, strategic development, customer-service and are the basis for reducing cost and maximizing returns.

1.2.2 Data must have clearly defined accountability.

Data are a by-product of business practice. Therefore, data owners, data stewards, and data custodians must control classification and use of data including change management.

1.2.3 Data must be seen as cross-functional, not siloed.

Data exists in an ecosystem of cross-functional dependencies where shared business practice knowledge is necessary for data processing and deployment.

1.2.4 Data integrity must be defined and managed consistently across the data life cycle.

Data must have defined business use validity, reliability, and quality from data entry to data retention.

1.2.5 Data must be managed to follow internal and external rules.

Security over data compliance and access to data is required to protect data of individuals and the institution.

[1] Data systems encompass Wichita State University ERP system-Ellucian Banner, non-Banner Enterprise systems and managed data systems including Business Intelligence and Predictive Modeling (BIPM), University Assessment Data Storage (UADS) and External Reporting Data (ERD). While largely dependent upon transactional databases (e.g., Banner), managed data systems are curated data configurations designed for ETLs, data quality audits, reporting and statistical analysis, and include data customizations, aggregation, imputation, forecasting, simulations, and AI related machine learning.

2. Data Governance Structures[2]:

2.1 Data Trustee (DT) Level

Data Trustees are executive level officers (i.e., President, Vice-Presidents) who have the authority to establish strategic planning priorities and reporting needs regarding data systems that impact functional users. They address disputes that arise from the Data Management Committee, provide resolutions, and can assign members where appropriate.

2.2 Data Management Committee (DMC) Level

The Data Management Committee is comprised of divisional units representing functional users who access data systems along with support groups that serve as a technical advising body. Membership is perpetual unless re-assigned by Data Trustees or vacancies.

Duties of the DMC include:

- Establish data governance policies and procedures as they relate to data systems.
- Identify data and reporting standards to meet the strategic planning priorities established by the Data Trustees.
- Assign security level access to data systems.
- Establish reporting metrics for consistency in information reporting.
- Manage metadata documentation of data systems including a glossary of reporting terms and assurance of data quality.
- Perform annual evaluation of data system components and functional user access.
- Share among committee members new and emerging business processes that impact data systems.

In addition to the above duties, the DMC can assign sub-committees and task forces as needs arise. DMC members can serve as data custodians. The Chief Data Officer serves as the DMC meeting moderator. DMC members are responsible for identifying Data Custodians within their divisional unit. The Office of Planning and Analysis (OPA), along with its technical support role, is responsible for meeting minutes and archiving DMC documentation.

Support groups serve to provide technical assistance to the DMC in terms of data/system operations and implementation of data storage, security, and reporting. While support groups are non-voting members in terms of data content and reporting standards, they can provide technical information on implementation feasibility and security. Serving as non-voting ex officio members, they may engage in discussion and make formal motions.

The DMC manages the metadata reporting term glossary which is to be publicly accessible to all university users of the managed data systems. The glossary serves to maintain clarity of reporting term usage and consistency across reports. The DMC also establishes single-source-of-truth (SSOT) and single-version-of-truth (SVOT) for metadata related data systems.

The DMC has no authority to change business practices or processes within units but can serve to provide recommendations to units on best practices and their impact on data reporting. The DMC shall report violations of security policy and may discontinue data access if found in material breach of policy.

Only DMC Data Owners and compliance officers have voting rights. In cases where a vote is required, all voting DMC members have one vote in which a simple majority defines the outcome. DMC voting members may request a second vote post discussion of the first vote. In the case of a tie vote, the issue goes to the Data Trustee level for resolution. A simple majority of data owners constitute a forum for voting.

DMC has the authority to call a Data Governance Council meeting which includes a full member roster of DMC (voting and support) and Data Custodian members. In addition, the DMC may elect to invite relevant Data Custodians or other university personnel to a DMC meeting. All deliberations and actions by the Data Management Committee including priorities and/or resolutions made by the Data Trustees will be made accessible from the Office of Planning and Analysis (OPA) including by-laws, organizational member chart, minutes, policies and procedures, glossary of reporting terms and contact information.

2.3 Data Custodians (DC) Level

Data Custodians play the role of data accountability within their functional area. Accountability comes in three dimensions:

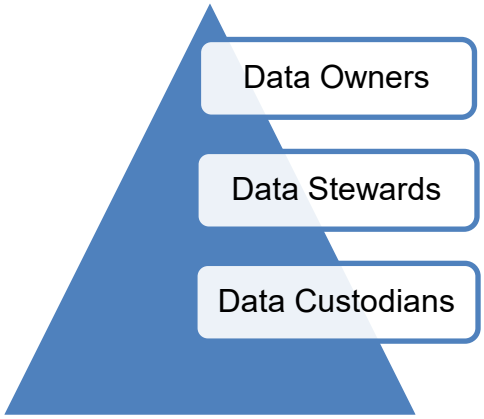
1) identification and correction of data entry errors identified by functional users and the DMC.
2) communicating to their DMC representative of new and emerging business practices that impact data and reporting.
3) advising the DMC of data source issues (e.g., discontinued data stores, preferred indicators) for managed data system builds

Data Custodians are nominated by their representative divisional DMC member and may be called to attend a DMC meeting as needs arise.

[2] WSU Data Governance (DG) structure is based on Best Practice within higher education as defined by Educause and leading universities in data governance (contact the Office of Planning & Analysis for a complete list of schools used to define WSU data governance structures).

3. Roles:

3.1 Data Governance Database Roles (individuals may occupy multiple roles):



Data Owner: data access

Data Owners oversee security access, use and content of data domains. Data domains are defined data storage elements typically segregated by functional area (e.g., finance, human resources, student). These data domains may cover a large set of functional offices that comprise data Stewards and data Custodians. For example, while the Registrar is the data Owner of student data (Saturn in the Banner System) for authorizing data access, the director of admission is the data Steward for the admission related tables as that person possesses the ability of have specific business practice knowledge related to that functional area.

Data Steward: data policy

Data Stewards establish data management policies related to functional offices for operational processing including security and reporting compliance. Data Stewards are business practice knowledge experts for their respective functional area and have the authority to make operational changes that impact data management and operational processing.

Data Custodian: data maintenance

Data Custodians oversee the deployment of policies established by the data Steward including data maintenance of operational transactional data systems. Their duties include data quality, integration of data with internal and external data systems, system upgrades, internal audit reporting, identification, and remediation of system failures.

4. C-Suite Related Roles and Coordinating Bodies

4.1 C-Suite Compliance Officers

Chief Data Officer (CDO) a senior-level compliance executive officer reporting to the Executive Vice-President and Provost.

Chief Data Officer oversees enterprise data governance, content, and use of all university enterprise data systems related to informational assets. **Data Governance** includes overseeing the establishment of data governance polices, data standards, reporting standards and coordinating the Data Council and Data Management Committees; working with Data Owners/Stewards/CIO/CISO to manage security access, compliance, and accountability**. Data Content** includes overseeing data quality, quality audits and accountability, data integrity, validity and reliability, identification of key performance indicators, overseeing implementation of new or modified software systems to ensure correct integration with university data systems, design, and development of data warehouses for reporting and analytics and vendor api data. **Data Use** includes overseeing reporting and deployment of reporting standards, security access to data sources, compliance with state and federal laws on data privacy, vendor api, development of advance analytics (descriptive, analytical, predictive, and proscriptive) and artificial intelligence.

Chief Information Officer (CIO) a senior-level compliance executive officer reporting to the Chief Finance Officer.

In addition to establishing operational standards and protocols, the Chief Information Officer oversees infrastructure, development, security, and services. **Infrastructure** includes overseeing data centers, networking, life cycle management, system integration, power systems and related redundancies, storage, archiving and recovery. **Development** includes application design and deployment, web-based systems, change management, data warehousing storage, enterprise reporting, and functional office programming. **Security** includes system and record level access security, identity management, and electronic facilities access. **Services** include desktop and device support, client IT configurations, IT purchases, device inventory, software licensing and deployment.

Chief Information Security Officer (CISO) a senior-level compliance executive officer reporting to the Chief Finance Officer.

Chief Information Security Officer oversees security governance, compliance, and monitoring. **Security** governance includes the creation of security policies and protocols, development of risk avoidance and compliance education. **Compliance** includes establishing protocols for compliance standards, reporting to internal-external agencies on compliance performance, working with university constituents to define and comply with identity management and record access. **Monitoring** includes overseeing efforts to identify information risk, establishing performance reports on security compliance and risk avoidance.

*The 3 C Suite roles: In layperson terms, a **CIO** builds and maintains a sandbox, the **CISO** constructs a fence around the sandbox and the **CDO** governs what happens in the sandbox.*

4.2 Coordinating Development and Advisory Bodies

Enrollment Services (ES)

Enrollment Services, charged by the president in 2014 to coordinate operational processing and strategic development among the core student functional offices of the Registrar, Admissions, and Financial Aid; Chief Data Officer is an at large member and only members have voting rights. Members hold Data Owner/Steward level policy making ability or oversite of university data governance (CDO). The Director of Enrollment Service convenes and moderates' meetings. The ES Director can invite other university office representatives to attend meetings as needed. New ES members can only be approved via a unanimous vote among current members and meet the standard of being a Data Owner/Steward. Primary ES objectives are to share current business practice knowledge across offices, coordinate new and modified data related systems, oversee change management on related enterprise systems, align operations to university and strategic enrollment management goals, ensure compliance practices are being enforced, develop and test data management initiatives (e.g., data retention policies), compile and provide curated data reports for strategic initiatives, and develop new initiatives that impact recruitment, enrollment and/or operational processes.

Enrollment Services is an extension of the DMC in allowing a focused team of core operational offices related to student admission, financial support, and enrollment to operate without burdening the larger body. ES oversees the primary line of business customers (students) which are classified as Master Data. In the event of a discussion or decision that would impact non-ES units or university data management policies, ES would be brought back to the DMC for discussion and final voting by the whole body.

Risk Advisory Committee (RAC)

The Risk Advisory Committee serves as an advisory body to the Data Management Committee on matters related to privacy, classifications, and regulatory compliance (including FERPA, HIPAA, NSPM-33 and others) of data. The RAC's mission is to identify, evaluate, and mitigate risks related to privacy, FERPA, HIPAA, and other security/compliance regulations and practices. Membership includes the Chief Data Officer, the Chief Information Security Officer and pertinent CISO staff, General Counsel, and Registrar. Duties include annually reviewing current data classifications including PII data inventory and university FERPA related directory information; evaluation of current data management initiatives and policies in development regrading compliance/risk; strategically develop policies, procedures, and standards to meet compliance and mitigate risk; provide to the Data Management Committee new or emerging developments in privacy/compliance and risk mitigation.

Technical Data Coordination Teams

The Office of Data Governance (ODG), Office of Planning & Analysis (OPA) and Information Technology Services (ITS) partner and coordinate the development, maintenance, security, and use of curated and university enterprise systems including university data management.

Office of Data Governance provides data scientists who develop and maintain the Business Intelligence & Predictive Modeling System (BIPMS), metadata (both business & technical) for university enterprise and BIPMS systems, data quality, data integration, data architecture, and data modeling and design.

Office of Planning & Analysis provides research analysts who extract and compile data from curated and university enterprise data systems for federal/state and other regulatory compliance reporting, university assessment and analysis, ad-hoc institutional requests, and manage data request security.

Information Technology Services provides server infrastructure, application development, enterprising reporting platforms, data warehouse storage, and system security.

5. Data Access and Transfer Authorization:

5.1 Data Owner Role in Data Access

Data owners play a key role beyond that of establishing data governance and policy over their data domains; they also manage who and for what purpose individuals or entities have access to data under their jurisdiction. Beyond authorized staff within their lines of reporting, whether persons or entities who ask for aggregate or record level data, data owners must authorize data access, ensure that the data provided aligns with the data request, and stipulate any restrictions on use or retention of data provided, including training if so noted.

5.2 Submitting Data Request

The Office of Planning & Analysis (OPA) serves as a central point of submissions for data requests, both aggregate and record level data. The OPA website (www.wichita.edu\opa) directs individual/entities who are seeking aggregate or record level data to the Data Request Form (DRF) (see Appendix B). Active students requesting data for research must have Institutional Review Board (IRB) approval. Aggregate data may have masked cell data (denoted by "<5") to protect the identity of an individual student or employee. Submitters are asked to complete a statement of intent that includes a declaration of:

- Reason for the data request and how the data are to be used or deployed.
- The target population
- What data fields are to be delivered?
- Who will have access to the data?
- Where and how will the data be stored
- Procedure for deleting the data once the project or task is complete.

Once OPA receives the DRF submission, it is forwarded to the appropriate data owner who may ask the submitter for clarifications related to the request. If the data owner authorizes the request, they will work with OPA to ensure the proper data are provided, any training that may be required of the submitter (e.g., Family Educational Rights and Privacy Act FERPA) and any compliance or data retention requirements. If the data request is denied, the submitter may appeal the denial decision by submitting an email to the Chief Data Officer who will forward the appeal justification and all related documents to the General Counsel Office.

If the DRF submitter is not an active student or employee, or is an active student or employee who is seeking data that will not be used for approved student research or tasks directly related to an employee's current job requirements, OPA will notify the submitter to seek approval from the General Counsel Office (www.wichita.edu/openrecords). If approved by the General Counsel Office, OPA will send the request to the appropriate data owner and assist in providing data as defined by the General Counsel Office. For non-university individuals/entities, or university active students or employees seeking data not related to approved research or their job requirements, who are not approved for data access by the General Counsel Office, see the General Counsel Office's appeal process.

5.3 Qualtrics and Survey Data

Qualtrics is the only institutionally authorized software for conducting surveys and is free of cost for eligible faculty, staff & students. The WSU Administrator within the Office of Planning and Analysis (OPA) serves as the central point of administration of Qualtrics Survey Software access and related survey data. The OPA website directs users to contact the Qualtrics WSU Administrator for access. The website also includes a survey Contact Request Form.

Accessing Qualtrics

To gain access to Qualtrics, users must be a current university employee, or an active student as indicated by the Banner data system. Students must have a faculty or staff advisor to set up a Qualtrics account. Qualtrics users must sign into the software through the Central Authentication Service and therefore must have a myWSU ID. Currently, WSU Tech employees are not eligible for Qualtrics accounts. The Qualtrics accounts of inactive employees and inactive students are deactivated each Fall semester.

Once an account is requested, the Qualtrics Administrator will send the user a registration survey in which they will provide personal contact information and the contact information of their faculty/staff advisor if they are using Qualtrics as a student. Upon receipt of the registration survey, the user's Qualtrics account is manually activated by the Qualtrics Administrator.

Requesting Data

Qualtrics contact lists requests can be made by eligible faculty, staff, or students. Students must have the permission of a faculty/staff advisor. To request a contact list, users must complete the Contact Request Form on the OPA website and submit it via email to the Qualtrics Administrator in OPA.

A contact list can be requested to distribute a survey to a large population of faculty, staff, and students affiliated with the university. Contact lists include first name, last name, and email address. The Contact Request Form asks for the following information:

- Reason for the data request and how the data are to be used or deployed
- The target population
- What data fields are to be delivered
- Who will have access to the data
- Where and how will the data be stored

Once the Contact List Request is received, the form is reviewed and approved at the discretion of the appropriate data owners. Once approved, the Contact List is uploaded to the user's Qualtrics account by the Qualtrics Administrator.

5.4 Third-Party Vendor Data Transfers

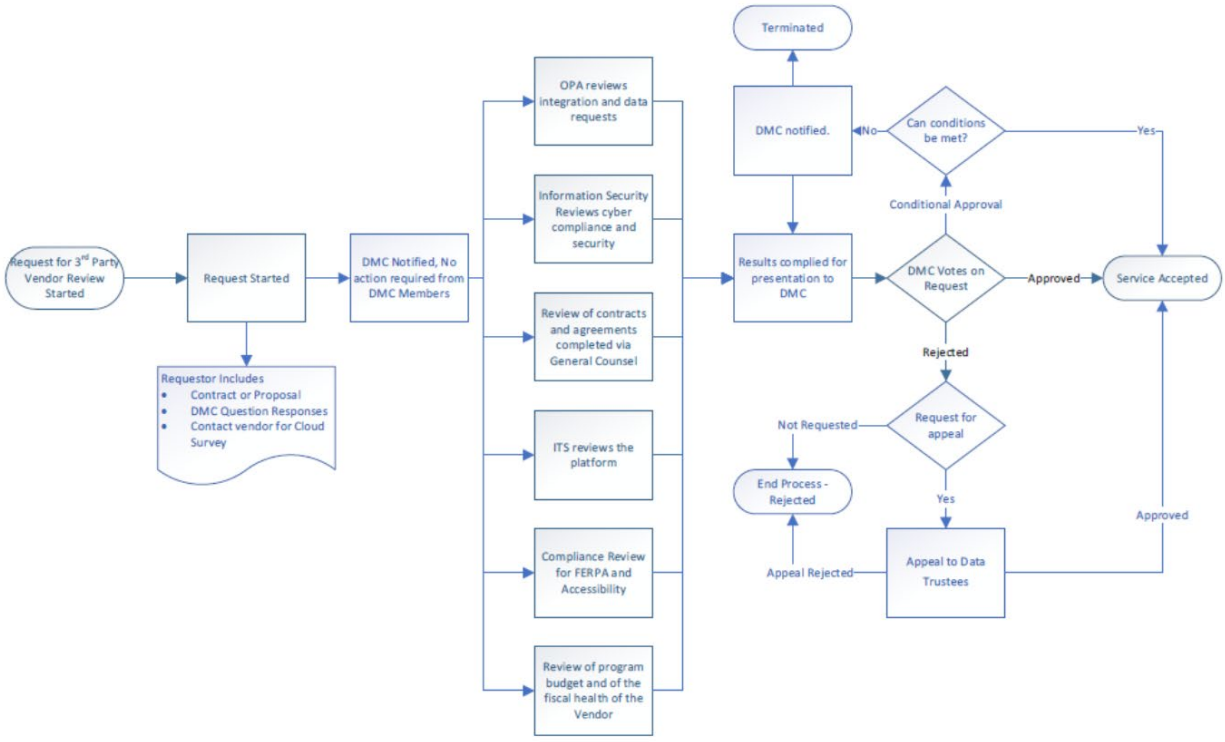
In accordance with university policy (19.18), the Data Management Committee is charged with reviewing any proposed contractual relationship with third-party vendors that involves the transfer of data from any enterprise information system, whether in aggregate or record level format, before the contract is finalized. Sponsored research related contract proposals are excluded from the review per policy (19.18). The contract proposal review applies to any new or renewal of third-party vendor data transfer relationships. This review is not a substitute for required department or management review of agreements. Departments such as General Counsel may leverage findings from DMC as part of their department processing.

The purpose of the Data Management Committee's review is to determine the following:

1. What is the problem/objective that is trying to be solved/addressed?
2. Does the proposed vendor solution fully address the problem?
3. Are there current contracts that provide a similar solution?
4. What is the data scope (population scope, data parameters to be delivered to vendor, number of potential records to be transferred, frequency of transfer)?
5. What Personally Identifiable Information (PII) related data is being transferred or stored by the vendor solution?
6. How will vendor flag for removal from use in the vendor platform the case of a person (e.g., student, employee) which should no longer be displayed in the platform (e.g., deceased, no longer active student or employee, has WSU trespass hold)?
7. How will the data be used by vendor and WSU staff?
8. Who will have access to the vendor solution, what data elements will they have access to, and have they been given clearance to view such data?
9. Can the data compilation and transfer be scaled appropriately and automated (e.g., is source data at WSU contained in Banner or other enterprise data systems)?
10. Does the proposed solution meet legal, policy and compliance requirements or have additional requirements as part of the implementation?
11. Have you created a post implementation review process to report whether the platform is meeting expectations including key metrics to track performance?
12. Has funding been secured for this project?
13. What is the expectation of when this project will be started and completed?

Units may submit their request for third-party vendor proposed contracts through the OPA website (to be determined). Submitters should allow a minimum of three weeks for DMC to complete their review barring time-delays related to vendor feedback.

Workflow of 3rd Party Vendor Data Transfer submission:



Excluded 3rd Party Vendor Services and DMC voting rights:

The institution has a limited subset of services that are excluded from voting for one or more of the following reasons:

- Legal encumberments as the institution is compelled to use the product or service.
- Requirements from the State of Kansas or Kansas Board of Regents
- Discontinuation of the service would be logistically infeasible as it is core to the basic operations of the institution with no viable alternative.

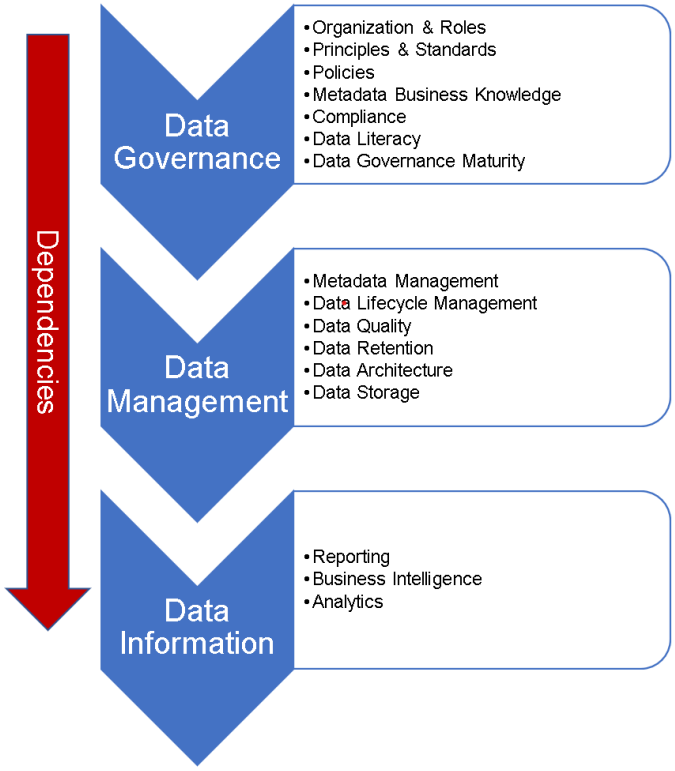
Excluded services shall be renewed following the same 3rd Party Vendor Data Transfer process, except there will be no vote taken. Additional controls and areas of risk may be noted and discussed. Excluded services require that after renewal review at the DMC, that the Chief Data Officer and Chief Information Security Office sign off in lieu of the DMC vote to express approval or disapproval for public record.

5.5 Vendor Out-Bound Data Inventory

Office of Data Governance is responsible for compiling an inventory of data that is transferred to 3rd Party Vendors including API job name, vendor, vendor platform, database source, table name, column data. These data are reviewed by the CISO office staff and Registrar to flag data elements that are PII, FERPA, HIPAA and other data classifications. Vendor data are reviewed annually and are part of the Third-Party Vendor Data Transfer review for new and renewal contracts.

6. Role of Data Governance: "Who's in Charge & Why"

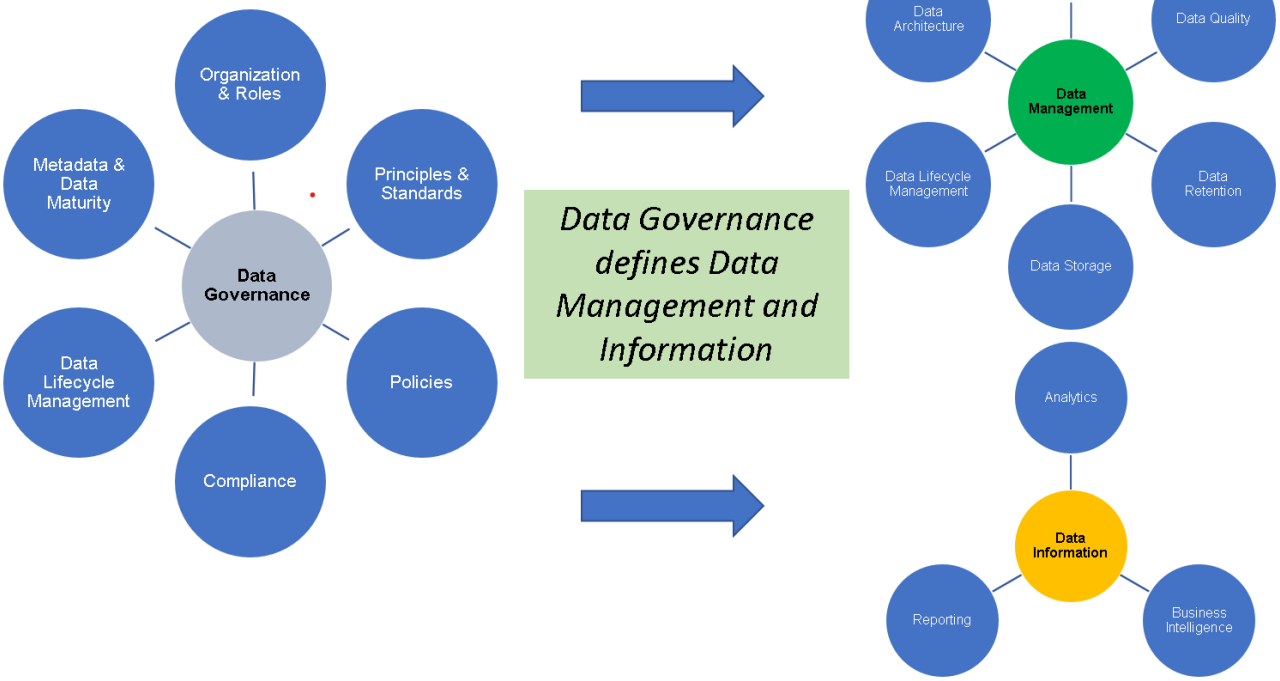
Data are assets which must be managed in service of business needs, not technology needs. Business defines what data are important, which data should be given data quality priority, defines what the data means, how long data must be retained, which cross-functional offices use the data, what's the business practice that creates the data. Once business metadata are defined, technology solutions (e.g., data quality, storage, analytics) can be implemented to automate data standards and curation for use.



Business-based Solution

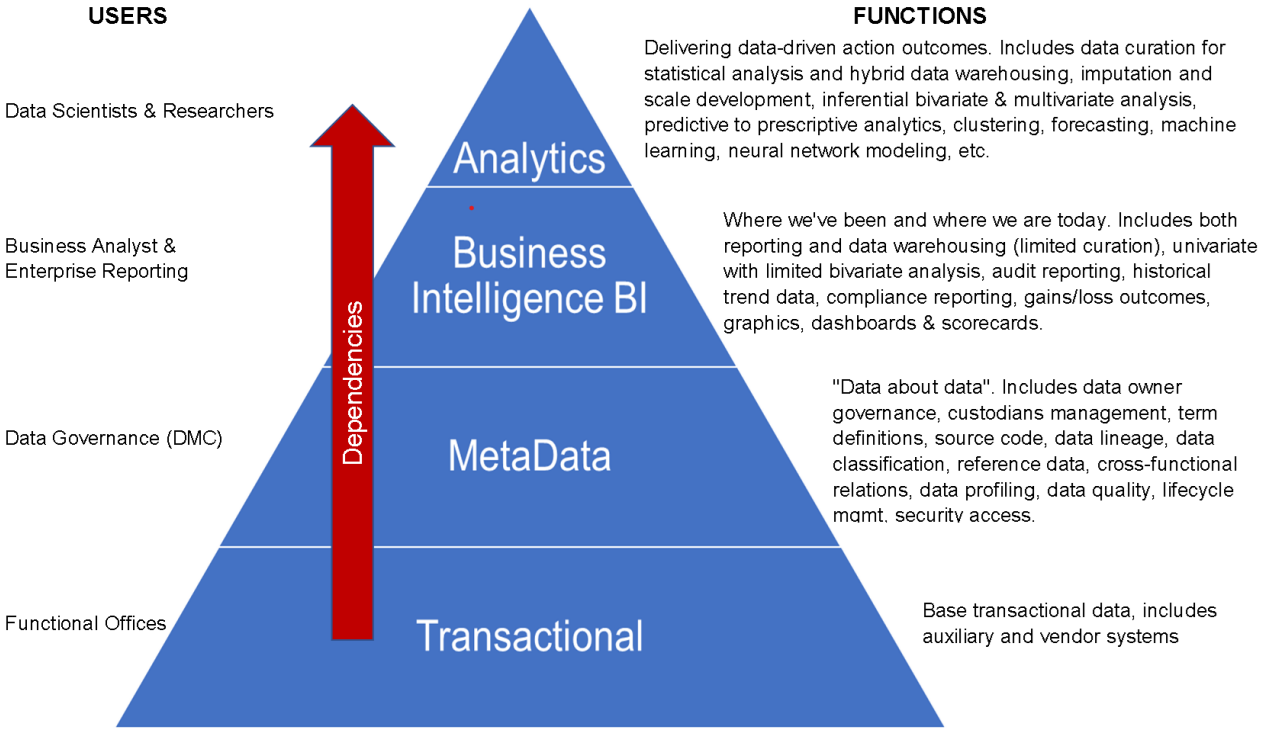
Technology-based Solution

Data as a valued enterprise asset that must be managed.

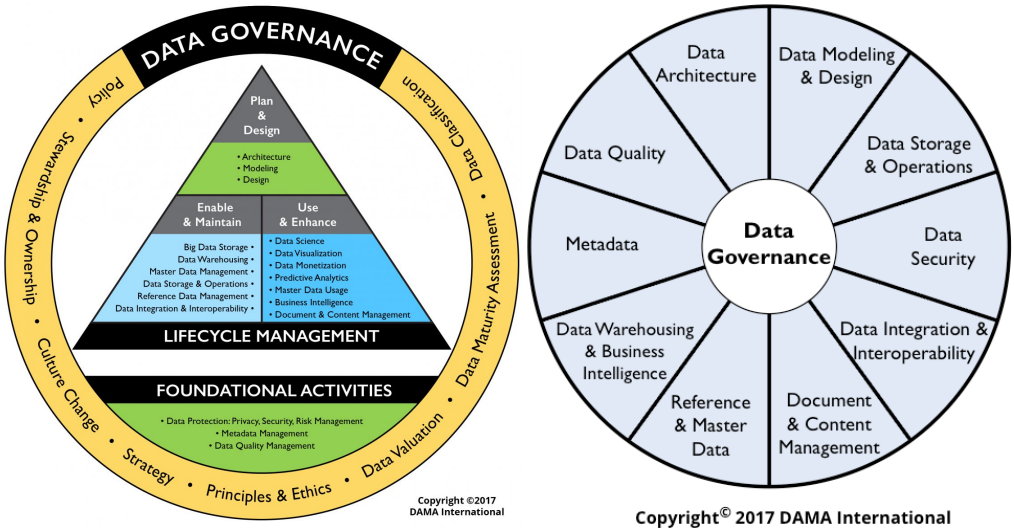


Because data are an asset that can be utilized indefinitely, even beyond the business transaction, data governance must extend to cover all facets including cross-functional use, reporting and analytics.

Data/Information Hierarchy and Dependencies



7. Data Management Activities Overseen by Data Governance Policies



7.1 Metadata Management: Details data ownership, cross-functional relations, business practice knowledge, terminology definitions, Key Performance Indicators (KPI) / Key Business Elements (KBE) [for both unit and enterprise needs], source code, reference data, logical and physical data structures and change management workflows.

7.2 Data Quality Management: Quality control management over defined data entry elements to ensure accuracy for business use and information integrity among cross-functional relationships. Includes determining data criticality (what data to audit), data profiling (anomalies, out of scope values, within scope values, distribution normality), root cause analysis and prevention, automated audit reports, and managing data quality over the data lifecycle.

7.3 Data Architecture: Articulation of data system components, relationships, dependencies, data flows and lineage of physical system infrastructure.

7.4 Data Modeling & Design: Articulation of data flows related to a business outcome (e.g., enrollment, degree completion), what and how data are related, data sources, and curation of data.

7.5 Data Storage and Operations: Documentation, procedures, workflows related to system maintenance and upgrades, backups, security access, and ongoing system performance monitoring.

7.6 Data Security: Security policies and procedures, proper authentication including Identify Access Management, preventative education, and ongoing monitoring.

7.7 Data Integration and Interoperability: Defined rules for ETL management, source code, load-balancing, monitoring to remove duplicate unique key records, management of semantic data element conversions across systems (source to storage to deployment),

7.8 Document and Content Management: Pertains to policies and management of data elements outside of physical systems including unstructured data. Includes lifecycle management, storage, access, index systems for classifications and information retrieval.

7.9 Reference and Master Data: Data elements that are used by multiple business units (e.g., contact information for address, phone, emails). Includes management of rules for common usage, security access, data quality management, and change management.

7.10 Data Warehousing and Business Intelligence: Establishment of rules and procedures for data storage to meet reporting and analytics needs across the enterprise. Includes managing storage optimization, minimizing data duplication, ensuring data integrity from source to data mart, data dictionaries and lineage mapping, provisioning data access, data lifecycle management including data retention.

APPENDIX A

(Original pdf on file, contact Office of Data Governance)

WICHITA STATE UNIVERSITY

OFFICE OF THE PRESIDENT

August 30, 2013
TO: David Wright
CC: Tony Vizzini, Gina Crabtree, Bobby Gandu, Lois Tatro, Vince Altum, Richard Muma, Jason Holmes, Jim Rogers, Tiffany Franks
FROM: John Bardo
RE: Data Management Task Force

The ability to make informed decisions, strategic planning, performance assessment and identify risk is contingent on having in place a well define data governance process that spans divisional units and addressesall university wide data information systems. For those information systems to be effective, we must have a collaborative representative body that oversees data quality, consistency in reporting and clarity of information terminology. In addition, it is important that this body provide guidance and recommendations on what serves the university best in business performance management and information supportive of strategic planning.

The body charged with these responsibilities is the Data Management Committee. The scope of this charge is inclusive of all data information systems (Banner and non-Banner systems) and must include a representative body of core functional leads across all divisions with support from technical units. In addition to the data governance processes, the Data Management Committee will serve as a recommendationbody to the university administrators for guidance on data information related issues and priorities.

The Data Management Committee, at a minimum will address the following duties:

- Share business knowledge and practices across units and divisions to optimize informationmanagement.
- Identify information that supports strategic planning initiatives as it relates to student success and operational efficiencies
- Provide guidance and recommendations on best-practice data information systems and processesincluding the evaluation of new business practices and data information delivery systems.
- Identify and resolve data quality issues.
- Create and manage the terms used for informational reporting so that reports are consistent, andterms are clearly defined.
- Provide easy and quick access of reports and information to university and community constituentswhile adhering to proper security access.

WICHITA STATE UNIVERSITY *Office of the President* [*1845 Fairmount Street* Wichita, *Kansas 67260*
tele (376) 978-3001 l *fax, (316) 978-3093* l *web, www.wichita.edu*