State of Indiana Policy: *Information Quality*

Version: 2.0 (12/2024)

Contents

State of Indiana Policy: *Information Quality*

Version: 2.0 (12/2024)

1. Purpose

The purpose of this Policy is to establish a robust framework that ensures the data managed by the State of Indiana is consistently fit for its intended use, driving data analytics, and fostering innovation. To achieve this, Indiana state agency staff are entrusted with specific roles and responsibilities for maintaining data quality.

By adhering to stringent data quality standards, the State seeks to guarantee the accuracy, completeness, and reliability of its data, thereby laying a strong foundation for evidence-based decision-making and the advancement of technological innovations, including artificial intelligence (AI) systems. This commitment to data quality is crucial for enabling data-driven policymaking and enhancing the efficiency and effectiveness of public service delivery. Through this Policy, the State aims to leverage high-quality data as a strategic asset to facilitate advanced analytics and support the development of reliable, innovative solutions that meet the needs of Hoosiers.

2. Applicability

This Policy shall apply to all Data as defined herein.

3. Revision History

Version	Date	Name	Revision Description	Supersedes
1.0	9/2017	B. Sirtosky	Initial version.	n/a
2.0	12/2024	J. Cooper M. Pradhan J. Stark	Wholesale revision. Aligns Policy with EDM Council frameworks.	1.0

4. Authority

This Policy is promulgated by the Office of the Chief Data Officer pursuant to IC 4-3-26-10(3). The OCDO may further promulgate component policies and/or subordinate standards, procedures, or guidance documents.

5. Definitions

1. "Data" means Government Information as set forth in IC 4-3-26-7.
2. **"**Data Collection" means a repository of Data collected from any source, by whatever means collected.
3. "Data Custodian" means an individual or entity responsible for the physical storage, protection, and accessibility of data, essentially managing the technical aspects of data storage and ensuring its security within a system, while not necessarily being involved in the data's definition or business rules.
4. "Data Owner" means an individual within an organization who is primarily responsible for the quality, accuracy, and integrity of a specific data asset within their domain, including defining policies, managing data access, ensuring compliance, and overseeing the data lifecycle management related to that data set; essentially, they are accountable for and hold decision-making authority over data assets.
5. "Data Quality Dimensions" are the metrics used to define the quality of the Data.

6. "Data Profiling" refers to the assessment of Data to understand its content, structure, quality, and dependencies.
7. "Data Stakeholder" means an individual within a state government agency who interacts with Data and is responsible for maintaining the quality and integrity of the Data they handle within the Data Collection. Data Stakeholders follow guidelines and processes established by Data Stewards and contribute to their agency's overall data quality initiatives. Data Stakeholders ensure the effective execution of data quality practices in their daily operations.
8. **"**Data Steward" means the individual that oversees agency data quality initiatives at a high level and prioritizes issues for resolution. A Data Steward has delegated responsibility for setting the overall strategic direction for Data Collections in an agency to ensure that Data Collections are developed, maintained, and utilized in accordance with applicable law, this Policy, and the strategic goals of the agency.
9. "DCAM Framework" means the Data Management Capability Assessment Model (DCAM), Version 2.2.3, put forth by the EDM Council.
10. **"**Metadata" means structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. The purpose of metadata is to add value to the Data it describes.
11. "MPH" means the Indiana Management Performance Hub established by IC 4-3-26-8.
12. "OCDO" means the Office of the Chief Data Officer established by IC 4-3-26-9.
13. "Policy" means this *State of Indiana Policy: Information Quality*.

6. Background

Through the daily operations of its agencies, the State of Indiana creates, maintains, and safeguards vast amounts of information relating to its citizens and the governing process. In electronic form, this information or "Data" is compiled into one or more Data Collections. This Data is an asset in providing government services to the public as well as informing the policymaking process to ensure the best outcomes for the Hoosiers we serve.

Ensuring that the Data is of the highest quality is of critical concern to the State of Indiana. Poor data quality can have a negative impact on interactions with the public, agency decision-making, and the overall efficiency of government operations. High data quality ensures that analytics, policy-making, and technological advancements such as artificial intelligence (AI) and machine learning (ML) are based on reliable, accurate, and timely information. Without high data quality standards, the trustworthiness of AI systems and the strategic decision-making process are compromised. This Policy is crafted to help ensure that Data across the State's agencies is consistently fit for purpose, trustworthy, and conducive to driving effective and informed decisions.

6.1 Data Management Capability Assessment Model (DCAM) Framework

A data management framework helps state agencies across the enterprise by:

- Setting clear, measurable expectations;
- Using metrics to quantify data management and pinpoint areas for improvement;

- Targeting improvement initiatives; and
- Ultimately demonstrating data management maturity, i.e. that data is fit for purpose and meets the specific needs of each business unit.

To ensure that sufficient data management frameworks are developed and implemented, the State of Indiana looks to best practices in the field of data management. The EDM Council, a recognized global leader in data management, provides the Data Management Capability Assessment Model (DCAM) Framework, which defines the scope of capabilities required to establish, enable, and sustain a mature data management discipline.

As it relates to data quality management, the DCAM Framework outlines a set of eight (8) components that allow an organization to effectively execute processes across its Data Collection, ensuring that the Data is fit for its intended purpose. The capabilities are categorized under the Foundation, Execution, Collaboration, and Analytics stages of data management. See visual aid and full list of Capabilities and Sub-capabilities in Appendix A.

The OCDO has adopted the DCAM Framework to assist in data governance, including data quality, efforts across the enterprise. In carrying out the OCDO Policy, MPH staff assist agencies in conducting DCAM assessments to assess their data management and governance maturity levels. More information on implementing the DCAM Framework for data management through the leadership of a Data Steward is described in Sec. 7.1.

Please note that the capabilities outlined in Sec. 7.2 are from Component 5 of the DCAM Framework and should be built upon Components 1-4, and continue through Components 6-8, as part of an agency's overarching data governance strategy. The Data Steward should consult with the OCDO as needed to ensure that this Policy is carried out effectively and efficiently.

6.2 Data Quality Dimensions

Data quality is a measurement of the degree to which the Data is fit for purpose and can be determined by evaluating it through a methodology that looks at defined measurements of data quality dimensions, defined below. Data quality dimensions are ways to categorize types of data quality measurements.

Having data quality dimensions is an integral part of a data quality framework and ensures consistent measurement of data quality across the enterprise. The dimensions identify important data quality aspects, enabling Data Stewards and Data Stakeholders to work together to: (1) define specific rules for what good quality data looks like in each area; and (2) set minimum acceptable levels for data quality, enabling the Data Steward or Stakeholder to track how well data meets these standards using clear metrics. By analyzing these metrics, data quality issues can be identified, and steps can be taken to improve.

The key quality dimensions defined by DCAM for data quality assessment are described below.

- **Accuracy:** a measurement of the conformity to facts of data to its authoritative source.
- **Completeness:** a measurement of the availability of required data attributes.
- **Conformity:** a measurement of the alignment of content with the required standards.
- **Consistency:** a measurement of compliance with required formats, values, or definitions.
- **Coverage:** a measurement of the availability of required data records.

- **Timeliness**: a measurement of the degree to which data is both representative of current conditions and available for use.
- **Uniqueness:** a measurement of the degree that no record or attribute is recorded more than once.

Finding a fitting set of dimensions and assigning quantifiable metrics to each based on your agency's business requirements is an integral part of a data quality framework as described in the following section.

Consult the ***OCDO Guidance: Data Quality Dimensions*** for more information about data quality dimensions.

7. Policy

Data quality is ultimately the responsibility of all state employees as they create, capture, and store Data in systems as a part of their official duties. To effectively manage data quality, and encourage agency alignment with the DCAM framework, the following additional roles and related responsibilities have been created.

7.1. Data Steward

Each agency must designate a minimum of one Data Steward but may have more than one assigned to one or more Data Collections. The Data Steward is responsible for meeting the defined component, capabilities, and sub-capabilities within the Data Quality Management component of the DCAM Framework. These responsibilities include, but are not limited to, the following:

1. Establish Data Quality Management (DQM):

- Consult on agency-specific DQM strategy outlining goals, processes, and resources.
- Assign roles and responsibilities for Data Stakeholders (data custodians, data owners, IT teams).
- Develop and document DQM processes for profiling, measuring, remediating, and monitoring data quality.
- Ensure DQM processes are auditable with clear documentation and record-keeping.

2. Profile and Measure Data:

- Identify critical data elements for quality assessment.
- Define data quality rules and metrics aligned with business needs that incorporate the relevant data quality dimensions described in Sec. 6.1. (Accuracy, Completeness, Consistency, etc.).
- Profile Data to understand its characteristics and identify potential issues.
- Analyze data quality reports to identify trends and areas for improvement.

3. Remediate Data Quality Issues:

- Prioritize data quality issues based on their business impact.
- Develop plans to address identified data quality problems (cleansing, correction, etc.).
- Track progress of data remediation efforts and report to Data Stakeholders.
- Identify root causes of data quality issues to prevent future occurrences.

4. Monitor and Maintain Data Quality:

- Establish data quality control points within data lifecycles.
- Continuously monitor data quality metrics to identify ongoing issues.
- Ensure data quality problems are being directed to and resolved by the relevant Data Stakeholders.
- Implement continuous improvement initiatives to enhance data quality over time.

Additional related responsibilities may include the following, as needed:

- **Front-end data validation.** Advocate for new systems to be built according to the conventions and standards referenced in this document as well as to have front-end data entry validation practices in place to help ensure conforming Data is entered into systems.
- **Employee training.** Ensuring that agency employees are adequately trained regarding data entry and the use of Data Collections.
- **Develop a RACI Matrix**. Responsible, Accountable, Consulted, and Informed documentation for all Data Stakeholders.

7.2. Data Stakeholder

A Data Stakeholder is an individual within an agency accountable for one or more aspects of data quality management. Data Stakeholders can be owners, custodians, IT support, data entry personnel, users or other roles associated with an agency's Data Collection(s) as identified and communicated by the Data Steward. There may be multiple Data Stakeholders within a given agency. Individual Data Stakeholders are assigned specific roles and responsibilities by the Data Steward in furtherance of the agency's DQM strategy. Data Stakeholders' responsibilities may include, but are not limited to, the following:

- **Exception reports/data profiling.** Implementing exception reports or data profiling that would identify where Data is missing, incomplete, or incorrect.
- **Business term glossary.** Creation and maintenance of a business term glossary that provides a common understanding of business terms and acronyms used within agency systems, reports, and documentation.
- **Naming conventions.** Creation and maintenance of database and application naming conventions that are used across agency systems and are consistent with the business term glossary.
- **Metadata Dictionary.** Ensuring each dataset has a corresponding data dictionary that includes all relevant metadata.
- **Data cataloging:** Ensure that all Data is scanned into the enterprise data catalog to facilitate accessibility, data lineage tracking, and governance. *See* Sec. 7.3
- **Front-end data validation.** Advocate for new systems to be built according to the conventions and standards referenced in this document as well as to have front-end data entry validation practices in place to help ensure conforming data is entered into systems.
- **Employee training.** Ensuring that state employees are adequately trained regarding data entry and the use of Data Collections.

- **Data standardization.** Standardizing Data as much as possible to promote uniformity in value and meaning.
- **Data cleansing.** Periodically cleansing and reconciling Data within and across Data Collections.
- **Data quality audits.** Periodically auditing systems to understand the degree to which data quality problems exist, identifying issues, and examining the health of the Data Collections regarding data quality standards established as part of the DQM strategy.
- **Corrective action.** Taking corrective action based upon data monitoring and audit results.
- **Report issues.** Escalating any issues to the Data Steward for resolution and consultation with the OCDO.

7.3. Enterprise Data Catalog

A foundational element of robust data quality management and governance is a data catalog. At current, the OCDO is in the process of deploying an Enterprise Data Catalog (EDC) for State Government through the Informatica platform. When directed by the OCDO, state agencies will be expected to scan Data Collections, capturing essential data source information in the process, to enable the creation and maintenance of a comprehensive, State-wide enterprise data catalog.

With respect to this Policy, this scan will include all metadata, including the following key attributes of scanned Data sources, as required by *OCDO Standard: Indiana Privacy Program Data Classifications*:

- Automated decision making questionnaire
- Granularity classification
- Privacy impact risk classification
- Security risk classification
- Records retention designation
- Regulatory classification
- Releasability questionnaire
- Storage location and trust questionnaire

Refer to the related standard via on.IN.gov/privacy for more information.

7.3.1 Access and Controls

The OCDO and the Management Performance Hub (MPH) are providing the EDC as a service to assist agencies with data quality and overall data governance. As such MPH will retain license to the product and set up all access, roles, and user controls for enterprise-wide implementation. MPH will provide user documentation, training materials, and support to agencies as they are onboarded into the EDC project.

Agencies will be able to view non-protected metadata from across the enterprise; however, an agency will not have the ability to export or modify metadata owned by another agency.

Access to the enterprise Informatica Data Catalog, where metadata assets are shared on an interagency basis, is only available to an employee or third party under contract with MPH. For the purposes of this provision, "employee" includes employees of the State of Indiana and individual temporary staffing resources designated through the Selected Resource Program under the Indiana Managed Service Provider program, Contract No.

58993. Access by other third-parties is subject to approval of or exception granted by the Office of the Chief Data Officer.

A third party under contract with an agency not the MPH may access metadata assets of the contracting agency within an approved "sub organization" - a smaller, distinct unit within the larger organization, allowing for separate management of user access, data, and settings - for the limited purpose and duration associated with data catalog implementation. However, post-implementation maintenance and operations shall be provided by an employee of the agency, the MPH, or third party contracted by the MPH.

7.3.2 Agency Title

Agencies will retain title to their metadata uploaded into the Informatica Data Catalog in accordance with IC 4-3-26-12. Further, neither the MPH, nor another agency with access, may fulfill requests for agency metadata under IC 5-14-3 (Access to Public Records Act) and will direct such requests to the owning agency.

7.4. Data Visualization

Agencies should ensure that all published data visualizations meet all best practices put forth by the OCDO in the upcoming ***OCDO Standard: Best Practices for Data Visualization*** (Release Date: TBD.) The scope of these best practices is to provide a tool agnostic, data visualization standard for agencies to reference and adhere to ensure visualization consistency, security, integrity, and quality. With respect to this Policy this includes ensuring the following:

- All published visualizations, both public and internal, have a defined and documented product owner.
- All published visualizations / have a defined and documented Data Steward, to ensure data quality is consistently monitored and maintained per the requirements of the agency's DQM strategy. (see Sec. 7.1)
- Public dashboards should have a defined refresh schedule that matches business needs.

Refer to the related standard via on.IN.gov/privacy for more information.

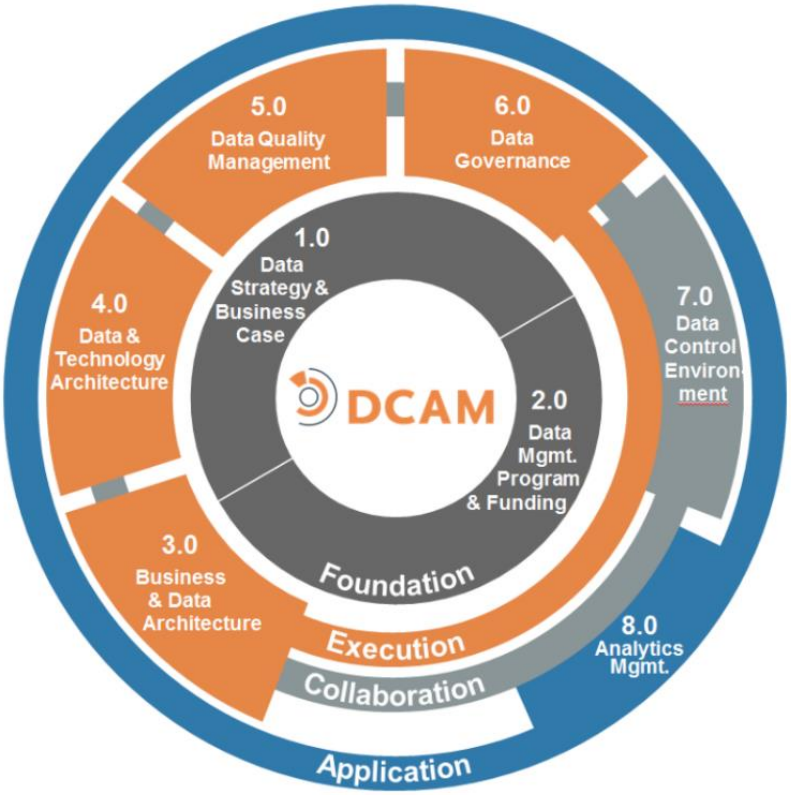
7.5 Data Quality Obligations for State Products

Notwithstanding obligations imposed by a Data Sharing Agreement, any marketing material put forth by a consultant or vendor, operating under a contract executed pursuant to IC 4-13-2 (the Indiana Financial Reorganization Act of 1947), referencing state products must be reviewed and approved by the owning agency to verify quality and appropriateness of data for publication use. Approvals provided longer than three months prior to publication will be considered invalid and a new review for approval will need to be conducted.

8. References

1. *DCAM Framework*, EDM Council, https://edmcouncil.org/frameworks/dcam/
2. State of Indiana Policy: *Information Privacy 2.0,* https://www.in.gov/mph/cdo/files/20230811-FINAL-State-of-Indiana-Information-Privacy-Policy.pdf .

DCAM Framework - Core Components Graphic:



DCAM Framework – Components, Capabilities, and Sub-capabilities List:

1.0 Data Management Strategy & Business Case

1.1 The Data Management Strategy (DMS) is Specified and Shared

1.1.1 The DMS is developed, documented, and consolidated

1.1.2 The DMS is aligned with high-level organizational objectives

1.1.3 The DMS addresses the core strategy concepts from each DCAM component

1.1.4 The DMS includes an established mechanism for approval

1.1.5 The DMS has been evaluated as being enforceable

1.2 The Data Management Business Case is Defined

1.2.1 High-level business requirements are documented

1.2.2 Business requirements have been prioritized, approved, and incorporated into the DMS

1.2.3 The DM business case is mapped to and aligned with the DMS

1.2.4 Expected DM outcomes are defined and sequenced

1.2.5 The DM business case is socialized and validated by stakeholders

1.3 The Data Management Vision is Defined

1.3.1 The Data Content Strategy is defined

1.3.2 The Data Usage Strategy is identified

1.3.3 The Data Management Deployment Strategy is communicated

2.0 Data Management Program & Funding Model

2.1 The Data Management Program (DMP) is Established

2.1.1 The DMP strategy and approach are defined and adopted

2.1.2 The DMP PMO is established and roles and responsibilities are defined and implemented

2.1.3 the DMP processes are defined and operational

2.1.4 The DMP has the authority to enforce adherence and compliance

2.1.5 The DMP concepts are reflected in the DMS

2.2 The DM Funding Model has been Established, Approved, and Adopted by the Organization

2.2.1 The DM funding model is matched to business requirements, implementation timelines, and operational capabilities

2.2.2 The DM funding model is aligned with the funding processes of the organization

2.2.3 Implementation of the DM funding model is enforced

2.3 The Data Management Organizational Structure is Created and Implemented

2.3.1 The Office of Data Management (ODM) is created

2.3.2 The ODM has an executive owner

2.3.3 The ODM is funded and staffed by individuals with the required skill-sets

2.4 The Roadmaps for the DMP are Developed, Socialized, and Approved

2.4.1 Program roadmaps are defined, developed, and aligned with the DMS

2.4.2 Program roadmaps are socialized and agreed to by stakeholders

2.4.3 Project plans are developed detailing deliverables, timelines, and milestones

2.5 Data Management Process Excellence Program is Established

2.5.1 DM process standards are defined and implemented organization-wide

2.5.2 DM processes are informed by industry standards and best practices

2.5.3 DM processes are supported by policy and auditable

2.6 Stakeholder Engagement is Established and Confirmed

2.6.1 Stakeholders commit and are held accountable for the DMP deliverables

2.6.2 Resource plans are aligned with and verified against initiative requirements

2.6.3 Funds are allocated and aligned to program roadmaps and workstreams

2.7 Communications and Training Programs are Designed and Operational

2.7.1 Internal communication plans have been defined and approved

2.7.2 Plans for communication with external regulatory bodies are defined and approved

2.7.3 Formal training programs have been defined and implemented

2.8 The DMP is Measured and Evaluated Against Business Objectives

2.8.1 Program metrics are defined and used to track progress

2.8.2 Outcome metrics are defined and used to track against business objectives

2.8.3 Process metrics are defined and used to drive continuous improvement

2.8.4 Financial metrics for total program costs and benefits (ROI) are tracked and reported

3.0 Business & Data Architecture

3.1 Data Architecture (DA) Function is Established

3.1.1 The DA strategy and approach are defined and adopted

3.1.2 The DA stakeholder roles and responsibilities are defined and implemented

3.1.3 The DA processes are defined and operational

3.2 Business Architecture (BA) is Integrated with Data Architecture (DA)

3.2.1 BA defines process input and output data requirements

3.2.2 Business data requirements must include data usage, data restrictions, and data ethics considerations

3.2.3 BA processes incorporate root cause fix of people or process

3.2.4 DA governance is aligned with BA governance

3.3 Identify the Data

3.3.1 Logical data domains have been identified, documented, inventoried, and authorized

3.3.2 Physical repositories of data have been located, documented, and inventoried

3.3.3 Physical data has been cataloged

3.4 Define the Data

3.4.1 Enterprise entities are identified, defined, modeled, and standardized

3.4.2 Business definitions are composed, documented, and approved

3.4.3 Unique identification and classification are defined, applied, and in use

3.4.4 Metadata is defined, modeled, and standardized

4.0 Data & Technology Architecture

4.1 Technology Architecture (TA) is defined in support of the data management initiative

4.1.1 DM is engaged in the Technology vision and strategy

4.1.2 DM is engaged in the definition and development of the organization-wide platform infrastructure

4.1.3 DM is engaged in the definition and development of the organization-wide data storage infrastructure

4.1.4 DM is engaged in the definition and development of the organization-wide data distribution infrastructure

4.1.5 DM governance is aligned with TA governance

4.2 DM Technology Tool Stack is Identified and Governed

4.2.1 DM technology tool selection strategy is defined and verified by stakeholders

4.2.2 Technology tool roadmap is developed and implemented

4.2.3 DM technology tool governance is integrated into Data Governance (DG**)**

4.3 Operational Risk Planning is in Place

4.3.1 Operational risk governance structure and processes are in place and implemented

4.3.2 Data infrastructure contingency planning is defined and in place

5.0 Data Quality Management

5.1 Data Quality Management (DQM) is Established

5.1.1 The DQM strategy and approach are defined and adopted

5.1.2 The DQM stakeholder roles and responsibilities are defined and implemented

5.1.3 The DQM processes are defined and operational

5.1.4 The DQM processes are auditable

5.2 Data is Profiled and Measured

5.2.1 Data has been identified and prioritized

5.2.2 Data Quality (DQ) rules are defined and tested

5.2.3 The data is profiled, analyzed, and graded

5.3 DQ Issues are Remediated

5.3.1 Data remediation has bene prioritized, planned, and actioned

5.3.2 Root-cause analysis (RCA) process is defined

5.4 DQ is Monitored and Maintained

5.4.1 DQ control points are in place

5.4.2 Data issues are managed

5.4.3 Continuous monitoring is performed

6.0 Data Governance

6.1 Data Governance (DG) Function is Established

6.1.1 The DG strategy and approach are defined and adopted

6.1.2 The DG organization structure is designed and implemented

6.1.3 The DG stakeholder roles and responsibilities are defined and implemented

6.1.4 the DG processes are defined and operational

6.2 Policy and Standards are Written and Approved

6.2.1 Policy and Standards are written and complete

6.2.2 Policy and Standards have been reviewed and approved by organizational stakeholders

6.2.3 Policy and Standards have been reviewed and approved by executive governing bodies

6.2.4 Policy and Standards are aligned with the organization-wide control function policy and standards

6.2.5 Policy and Standards are enforceable and auditable

6.3 Govern the DM Program

6.3.1 Program funding governance is established and operational

6.3.2 Program and project review and approval processes are established

6.3.3 Business process optimized for DM is enforced

6.3.4 Issue management process is defined and operational

6.4 Govern the Data Structure

6.4.1 Govern the Authoritative Data Domains identification and use

6.4.2 Govern the models, glossaries, identifiers, classifications, and relationships

6.5 Govern that the Data is Fit-for-Purpose

6.5.1 Govern the data access and use

6.5.2 Govern the adherence to contractual terms & regulatory policy

6.5.3 Govern the data use according to established Data Sharing Agreements

6.6 Govern the Data Ethics

6.6.1 Establish a formal data ethics oversight function

6.6.2 Govern the ethical access and appropriate use of data

6.6.3 Govern the ethical outcomes of data access and use

7.0 Data Control Environment

7.1 Data Control Environment (DCE) is Evidenced

7.1.1 The Data Control Environment is established

7.1.2 The stakeholder roles and responsibilities are defined and implemented

7.1.3 DM capabilities are aligned and working collaboratively across the organization

7.2 Cross-organization Control Function Collaboration

7.2.1 Control function and data management policies and standards are aligned

7.2.2 Regular routines are established with cross-organization control functions

7.2.3 Data entering the ecosystem is subject to cross-organization controls

7.3 Data Risk is Managed

7.3.1 Organizational Unit compliance

7.3.2 Data Risk function oversight

7.3.3 Internal Audit review

8.0 Analytics Management

8.1 The Analytics Function is Established

8.1.1 The Analytics strategy and approach are defined and adopted

8.1.2 A categorization system for levels of analytics is defined and adopted

8.1.3 The Analytics operating model is defined, and its structure is implemented

8.1.4 The funding model for Analytics has been established, approved, and adopted

8.1.5 Analytics governance structures are in place

8.1.6 An analytics methodology and model documentation standard have been adopted

8.2 Analytics is Aligned with Business and Data Management Strategy

8.2.1 Dependencies between Analytics and Business Architecture are understood and addressed

8.2.2 The prioritization of Analytics is driven by business strategy

8.2.3 Analytics support and influence business needs and is actionable where required

8.2.4 Analytics impact is measured and understood to be driving business value

8.3 Analytics is Aligned with Data Architecture

8.3.1 Analytics data lineage is understood, and authoritative data sources are used

8.3.2 Analytics reference approved business definitions

8.3.3 Analytics respect the organization's identification and classification standards

8.3.4 Data preparation standards exist and are applied consistently

8.4 Analytics is Aligned with Data Quality

8.4.1 The quality of data both used and created by analytics is fit-for-purpose

8.4.2 Issues identified during data preparation are managed via the Data Quality Management framework

8.5 The Analytics Platform is Designed and Operational

8.5.1 The platform design meets the needs of the Analytics operating model

8.5.2 The platform addresses the separate needs for innovation and production

8.5.3 A version control regime is defined and in place

8.5.4 Data obfuscation strategies are defined and supported

8.5.5 Environment scalability requirements are understood and appropriately supported

8.6 Model Operationalization is Established

8.6.1 Model testing, approval, release, and regular review processes are in place and effective

8.6.2 Model approval and release is aligned with data ethics governance

8.6.3 Model approval and release is aligned with privacy governance

8.6.4 Model bias is understood and managed

8.6.5 Requirements for model explainability are understood and incorporated

8.7 The Analytics Culture and Education Needs are Managed

8.7.1 The behaviors needed for an Analytics culture are understood and measured

8.7.2 Initiatives to address culture gaps are in place

8.7.3 The learning experience needs of Analytics practitioners are defined

8.7.4 Education initiatives to address skills gaps are in place