سلطنة عُمان
وزارة النقل والاتصالات وتقنية المعلومات
Sultanate of Oman
Ministry of Transport, Communications and Information Technology

نتقدم بثقة
Moving Forward with Confidence

رؤية عُمان 2040
OmanVision

National Data Governance and Management Compliance Assessment Model

Document Control

Version	First
Date	2024
Author	Ministry of Transport, Communications and Information Technology

Issuance and Publication

Issuing authority	General Directorate of Polices and Governance
Email	governance@mtcit.gov.om
Date of Issuance	2024

Distribution list

1	All units of the State's Administrative Apparatus.
2	Regulatory bodies for various sectors

Table of Contents

1.0 Introduction

The Sultanate of Oman, aligning to the objectives of vision 2040, has planned several strategic digital transformation programs for driving economic growth, innovation, and public welfare.

As a significant step in this direction the National Data Strategy was published by the National Center for Statistical Information (NCSI) via resolution no. 2022/103. Article (40) of the National Data Strategy entrusts the Ministry of Transport, Communications, and Information Technology (MTCIT) with the following responsibilities:

- 'Preparing policies and standards for data management and governance and following up on the commitment of units of the state's administrative apparatus and other public legal persons to these policies.'
- 'Preparing the necessary guidelines and guides to support the application of policies and standards.'
- 'Preparing and presenting awareness workshops for units of the state's administrative apparatus and other public legal persons.'
- 'Adopting initiatives based on technical data and coordination between beneficiaries from the government and private sectors.'
- 'Preparing and supervising the implementation of open data programs.'

Further for MTCIT to undertake the assigned responsibilities by the National Data Strategy and to resolve the challenges faced earlier by the government sector in complying with multiple existing data management laws/policies/frameworks and guidelines, the Ministry has developed the National Data Governance Framework to empower the implementation of the National Data Strategy and provide a unified, structured, and comprehensive approach towards managing and regulating data.

The diagram below showcases the sequence of events leading to the development of the framework.

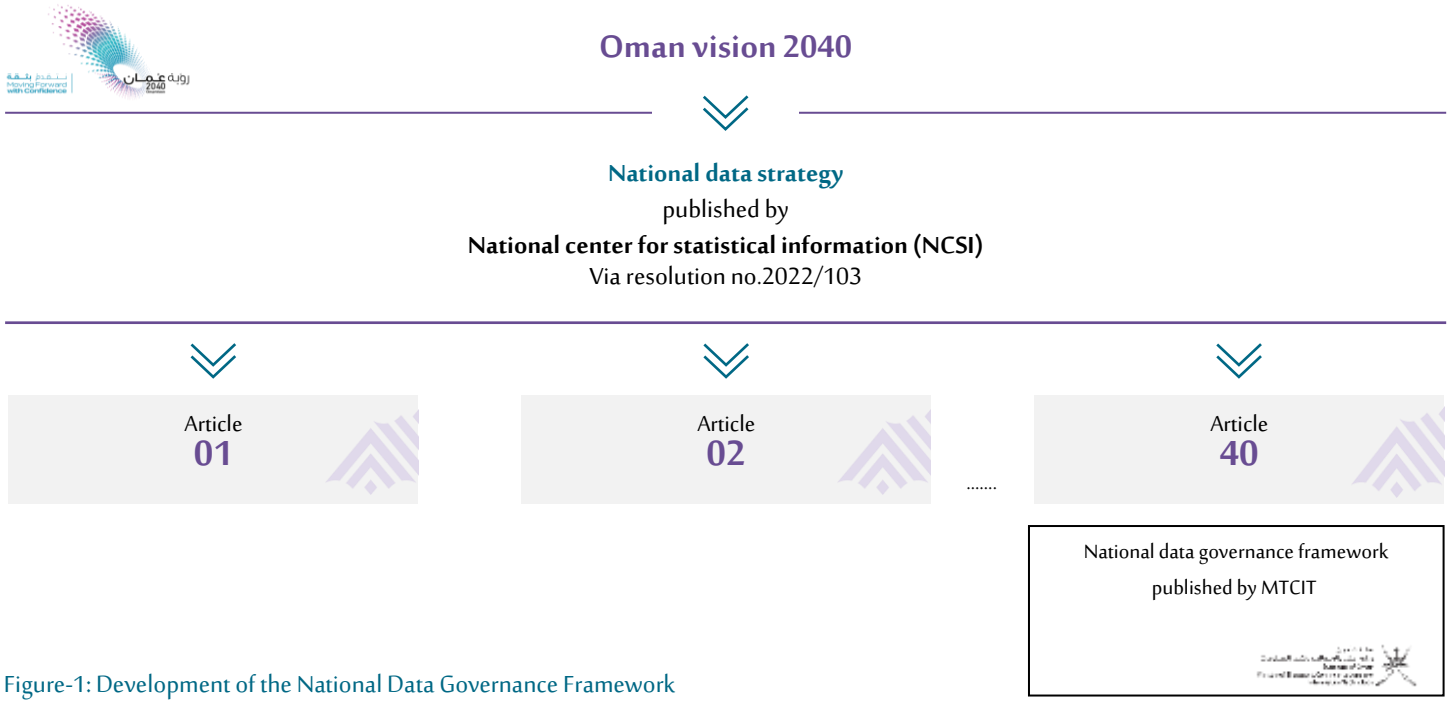


Figure-1: Development of the National Data Governance Framework

The framework consists of 3 components providing the necessary requirements for data governance and management across 14 domains. Together, the 3 components will ensure the establishment of robust data governance and management practices across the government entities within the Sultanate of Oman. A brief description of the 3 components is provided below:

National Data Governance Framework

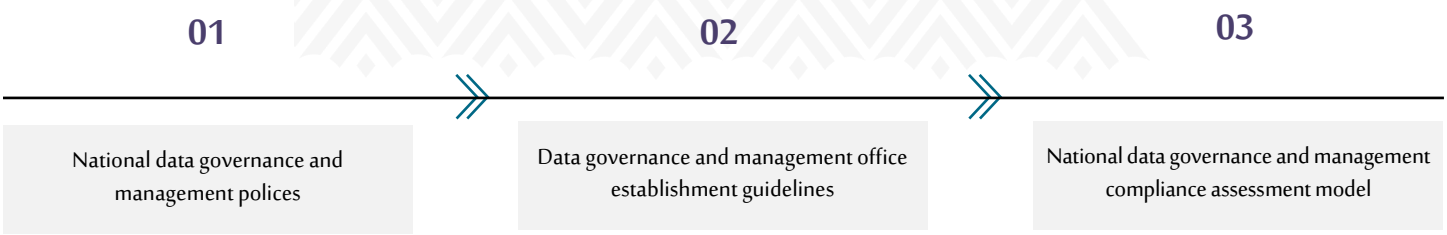


Figure-1: National Data Governance Framework Ecosystem

- **National Data Governance and Management Policies** – The policies outline the necessary requirements across 13 out of the 14 data governance and management domains to establish a robust data governance practice within the government entities. The Document and Content Management domain will be covered by the existing policies/laws developed in the sultanate.
- **Data Governance and Management Office Establishment Guidelines** – The guidelines provide the necessary elements to support the government entities for establishing their Data Governance and Management Office including the mandate, services and processes, organization structure, roles, and responsibilities, positioning within the entity and governance model.
- **National Data Governance and Management Compliance Assessment Model -** The model outlines the compliance assessment methodology, the implementation priorities, and the assessment criteria for enabling the government entities to comply with the national data governance and management policies.

Specifically, the National Data Governance and Management Compliance Assessment Model aims to establish a standard approach to assess the compliance of the government entities with respect to the National Data Governance and Management policies and is pivotal towards realizing MTCIT's overarching data governance vision of establishing data as a foundation for the Sultanate's economic growth objectives.

This document should be read in conjunction with the National Data Governance and Management Policies and Data Governance and Management Office Establishment Guidelines for a comprehensive view of the National Data Governance Framework requirements.

1.1 Data Governance Vision and Mission

Data as a key enabler for decision-making and leading economic development in the Sultanate of Oman

Activate an effective national data governance framework that fosters collaboration between data owners and end users, through setting clear directions with the required level of policies for managing and governing data, adopting best practices, and ensuring continuous compliance, in order to reposition data as a driving force for the national economy.

Figure-2: National Data Governance Vision and Mission

1.2 Data Governance Principles

The National Data Governance framework is based on guiding principles which have been identified based on leading international best practices. The data governance guiding principles have been formulated in alignment with the vision and mission for Oman's data governance framework.

Data is a national asset
Develop practices that enable realization of the inherent value of data as a national asset to drive innovation and unlock economic growth through data integrity, monetization, transparency and accountability. **01**

A data-driven culture is encouraged
Establish processes and develop skills required for entities to utilize their data, derive meaningful insights and leverage technology to improve their decision making and operational efficiency. **02**

Data is shared and is available on time
Develop practices to facilitate seamless internal and external sharing of data, ensuring that data users obtain information in a timely manner, thereby improving the quality and efficiency of decision-making processes. **03**

Data is trusted by all stakeholders
Establish practices for providing reliable, accurate and fit for purpose data to build data trust and confidence thereby, facilitating informed decision making. **04**

Data is understood uniformly across all stakeholders
Establish practices that enable a uniform understanding of the data to facilitate efficient data exchange and analysis thereby promoting reliability and efficiency in utilizing data assets within the entity. **05**

Data practices are compliant with regulatory requirements
Develop data governance and management practices that uphold the regulatory requirements to ensure lawful, ethical and responsible handling of data across the business processes of the entities. **06**

Data is managed across its lifecycle as per business needs
Develop practices that help collect, store, dispose/archive data as per its relevance and purpose along with delivering it to the data consumers. **07**

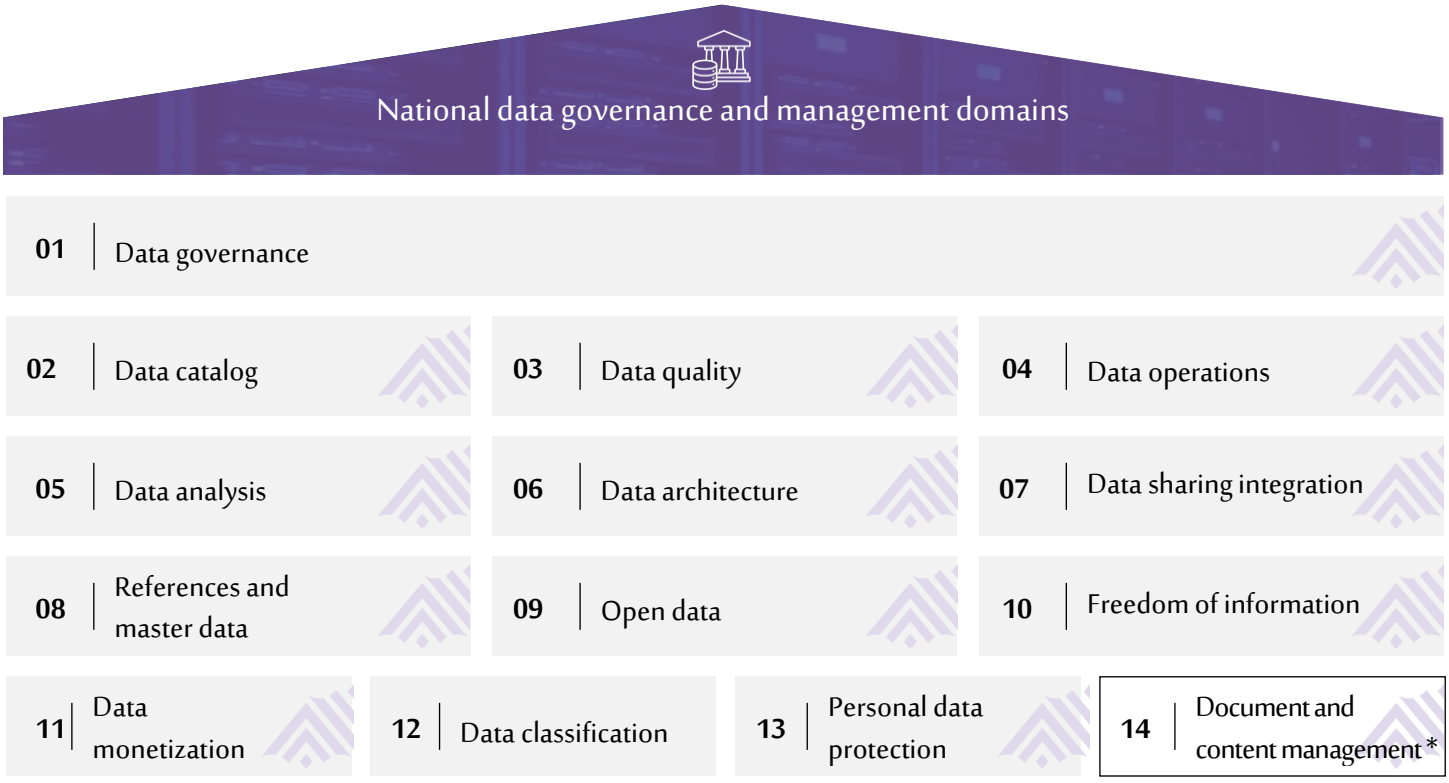
Figure-3: National Data Governance Guiding Principles

2.0

Scope and Applicability

2.0 Scope and Applicability

The scope of the National Data Governance and Management Compliance Assessment Model covers 13 data governance and management domains. The below diagram showcases the domains in scope for the National Data Governance and Management Compliance Assessment Model.



* Document and content management domain will be covered by the existing domain specific/lows

Figure-4: National Data Governance and Management Compliance Assessment Domains

3.0

Compliance Assessment Methodology

3.0 Compliance Assessment Methodology

3.1 Overall Approach and Phases

The compliance assessment methodology consists of six phases, aimed at establishing a standardized process for MTCIT to assess compliance of the government entities to the National Data Governance and Management Policies.

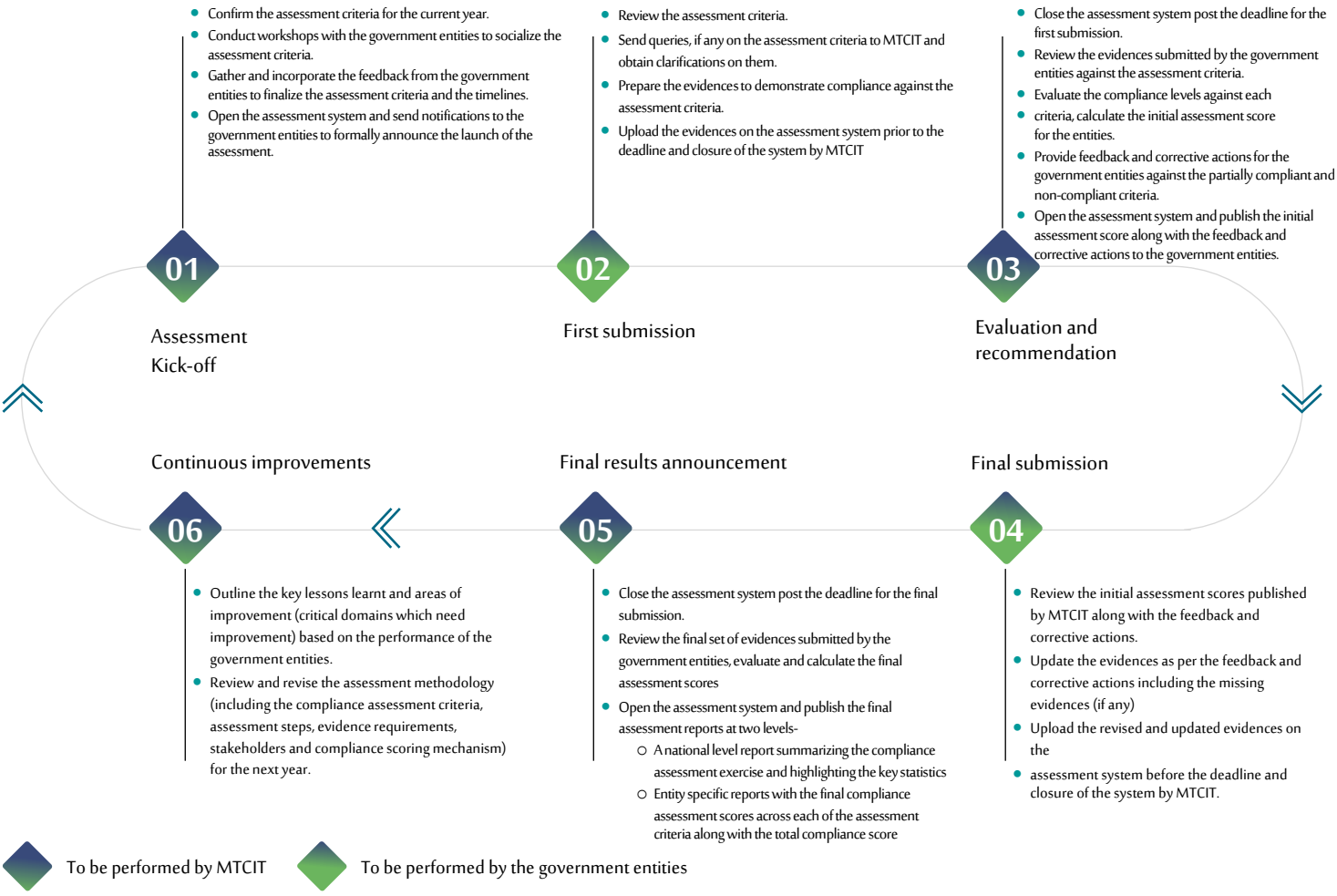


Figure 5: Compliance Assessment Phases

3.2 Scoring Methodology

A standardized scoring methodology shall be applicable to assign a quantitative measure for the degree of compliance to the National Data Governance and Management Policies across the government entities.

The scores shall be calculated at 4 levels of hierarchy. The following diagram depicts the 4 levels:

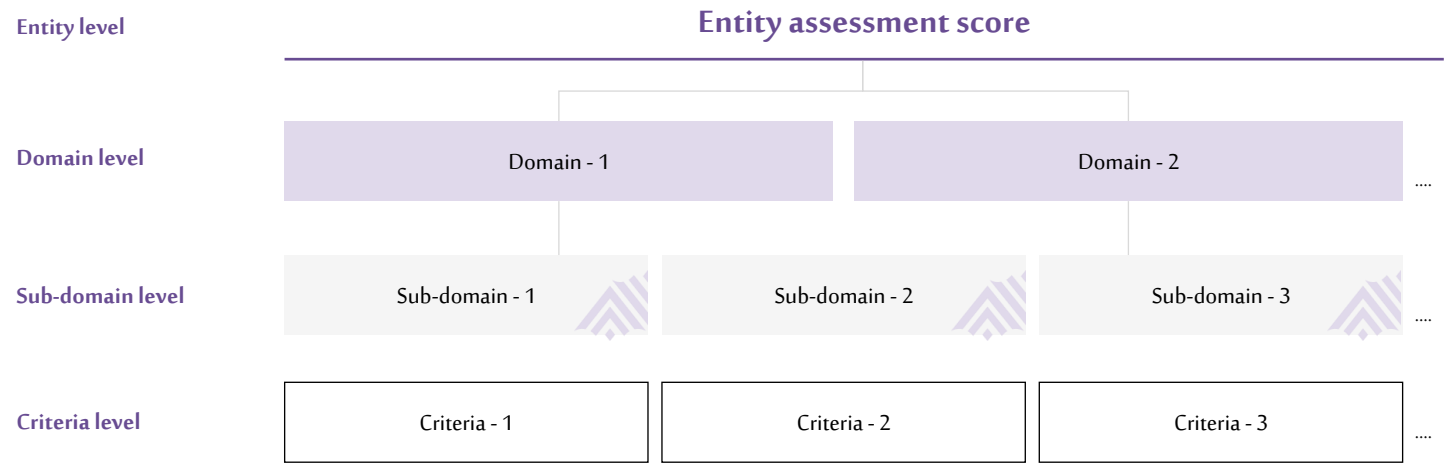


Figure 6: National Data Governance and Management Compliance Scoring Hierarchy

- **Entity Assessment Score**

  The entity assessment score shall be calculated as the average of all the domain level scores. The entity assessment score denotes the final compliance score of the entity as per the National Data Governance and Management Policies.

- **Domain level**

  The domain level score shall be calculated as the average of the scores obtained for all the sub-domains under the domain.

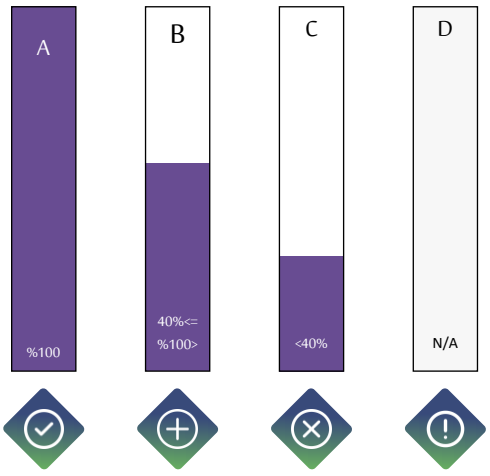
- **Sub-domain level**

  The sub-domain level score shall be calculated as the average of the scores obtained for all the applicable criteria under the sub-domain.

- **Criteria Level**

  At the criteria level, every criterion shall have an appropriate level of compliance assigned as per the evidence produced.

To monitor the degree of compliance to the assessment criteria, 4 levels of compliance have been defined which have been described in the following figure:



A. Fully compliant

The entity demonstrates complete coverage of the criterion within the produced evidence(s)

B. Partially compliant

The entity demonstrates compliance to at least 40% of the criterion but not complete coverage withing the produced evidence(S)

C. not compliant

a criterion shall be termed "not applicable" for an entity, if it submits the reason and obtains approval from MTCIT for the criterion to not be applicable

D. non-compliant

The entity fails to demonstrate compliance to any of the criterion terms within the produced evidence(S) or produces no evidence against a particular criterion

Figure 7: National Data Governance and Management Compliance Assessment Levels

MTCIT has the discretion to assess the evidence provided by the entities and determine if it qualifies as partially compliant or non-compliant.

For each level of compliance, a score shall be assigned. The figure below showcases the applicable scores to each level of compliance.

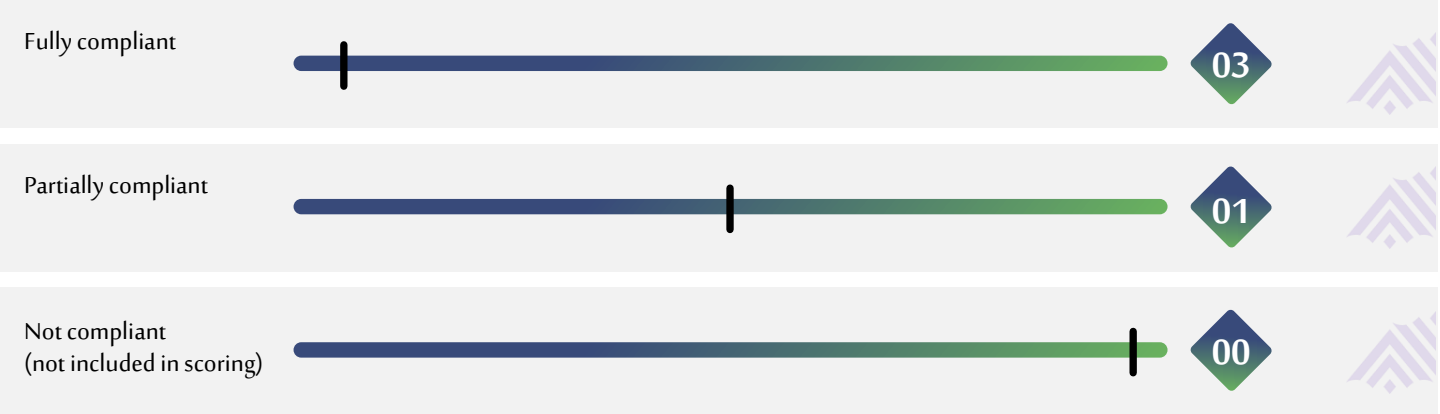


Figure 8: National Data Governance and Management Compliance Assessment Level Scores

Explanation with an example:

Take the example of the criterion DG.2.3. (Please refer to Section 4 of this document for the criterion and corresponding evidence required):

A governance model shall be established for the data governance and management office for governing its operations and handling the data governance related issues arising within the entity. The governance model, at minimum, shall include the following:

- Data Governance Committee – To set the strategic direction for data governance and management program within the entity.
- Data Governance and Management Working Team – To implement the data governance and management policies and related practices across all business units within the entity.

As per the evidence outlined for DG.2.3, an entity can become "Fully Compliant" for this criterion if it provides all the three evidence (100%), whereas if it provides any two of the three evidence (66%), then the entity will become "Partially Compliant" for this criterion. Additionally, if the entity provides only one evidence (33%), then it becomes "Non-Compliant".

3.3 Prioritization Plan

The National Data Governance and Management Policies (criteria) are assigned with priorities to enable standardized implementation timelines and support the government entities to strategize and plan their data governance programs. The priorities are divided into 3 categories, namely Priority-1, Priority-2, and Priority-3.

The below section provides an overview of the priorities of the criteria mapped to the implementation timelines:

- **Priority 1**
  The Priority 1 criteria shall be implemented by the government entities within the first year of the release of the National Data Governance Framework.
- **Priority 2**
  The Priority 2 criteria shall be implemented by the government entities from the second year of the release of the National Data Governance Framework.
- **Priority 3**
  The Priority 3 criteria shall be implemented by the government entities from the third year of the release of the National Data Governance Framework.

4.0

Compliance

Assessment Criteria

4.0 Compliance Assessment Criteria

This section outlines the policy statements of the National Data Governance and Management Policies in the form of standardized acceptance criteria to demonstrate compliance across 13 data governance and management domains for all the government entities of the Sultanate of Oman, thereby simplifying the evaluation process and enhancing transparency. The following section maps the defined criteria to the evidence necessary for demonstrating compliance along with the implementation priorities.

4.1 Data Governance (DG)

DG.1 Data Management Strategy and Plan

Policy Number	Criteria	Priority	Evidence
DG.1.1	The entity shall assess its data governance and management capabilities to identify the gaps and initiatives to be implemented for compliance to the National Data Governance Framework.	P1	• Data governance and management assessment report outlining the gaps and recommended initiatives.
DG.1.2	A data management strategy shall be established in alignment to the entity's strategic business objectives. The strategy, at minimum, shall include the following: • Data governance and management vision, mission, and guiding principles. • Initiatives across the data governance and management domains. • Key performance metrics to continuously monitor execution of the data management strategy. The entity shall obtain approval of the data management strategy from the entity's data governance committee.	P1	• A documented and approved data management strategy. • Minutes of meeting of the entity's data governance committee providing approval on the data management strategy.
DG.1.3	A data management strategy execution plan shall be developed to implement the data management strategy. The plan, at minimum, shall include the following: • Data management projects and scope. • Estimated budget for data management strategy execution plan implementation. • Key risks and its corresponding mitigation plan. • Key success factors. The entity shall obtain approval of the data management strategy execution plan from the entity's data governance committee.	P1	• A documented and approved data management strategy execution plan. • Minutes of meeting of the entity's data governance committee providing approval on the data management strategy execution plan.
DG.1.4	The approved data management strategy and the data management strategy execution plan shall be maintained and published on the internal portal of the entity.	P1	• Screenshot of the approved data management strategy and execution plan maintained within the internal portal of the entity.
DG.1.5	The data management strategy execution plan shall be periodically reviewed and updated. The entity shall document the outcome of the periodic review along with outlining any changes made.	P2	• Data management strategy review register containing information of review observations, the recommended and approved changes along with the version history. • Minutes of meeting of the entity's data governance committee providing approval on the updated data management strategy execution plan.

DG.2Data Governance and Management Organization

Policy Number	Criteria	Priority	Evidence
DG.2.1	The entity shall establish a data governance and management office to operationalize the entity's data governance strategy.	P1	• Organization structure document including the data governance and management office. • Formal approval from the HR or equivalent department on the organization structure document which includes the data governance and management office.
DG.2.2	The entity shall establish data governance roles to entrust the accountability and responsibility of operationalizing the initiatives of the data governance strategy. The data governance roles, at minimum, shall include the following: • Data Governance and Management Head • Data Management Officer • Data Governance and Compliance Officer • Data Owners • Business Data Stewards • IT Data Steward • Enterprise Data Architect • Data Protection Officer	P1	• A documented and approved role mapping document, detailing the alignment of employee names with their respective roles along with the responsibilities outlined in the 'Data Governance and Management Office Establishment Guidelines'. • Formal approval of the role mapping document along with responsibilities, from a competent and recognized authority within the entity (For e.g. Head of Entity, HR Head).
DG.2.3	A governance model shall be established for the data governance and management office for governing its operations and handling the data governance related issues arising within the entity. The governance model, at minimum, shall include the following: • Data Governance Committee – To set the strategic direction for data governance and management program within the entity. • Data Governance and Management Working Team – To implement the data governance and management policies and related practices across all business units within the entity.	P1	• Documented and approved data governance charter outlining the establishment of a governance model for the data governance and management office in alignment with the 'Data Governance and Management Office Establishment Guidelines.' • Evidence of approval from the Head of the Entity on the data governance charter (e.g. email, minutes of meeting etc.). • At least 3 documented minutes of meeting of the data governance committee and data governance and management working team meetings outlining at minimum, the agenda of the meeting, meeting participants and the discussion points.
DG.2.4	The entity shall document and maintain the decisions taken by the data governance committee along with its approval.	P1	• Documented and approved data governance data register. • Minutes of meetings outlining at minimum the meeting participants, discussion points along with the approval for each of the decisions taken by the data governance committee.
DG.2.5	The entity shall periodically monitor and track the performance of its data governance and management office.	P2	• Documented and approved report outlining the performance of the data governance and management office as per the Performance Indicators defined in the 'Data Governance and Management Office Establishment Guidelines' and measured as per the defined time period. • Minutes of meeting of the entity's data governance committee providing approval on the report outlining the performance of the data governance and management office.

DG.3 Data Governance and Management Policies and Processes

Policy Number	Criteria	Priority	Evidence
DG.3.1	The entity shall develop entity specific data governance and management policies in alignment with the 'National Data Governance and Management Policies' covering the data domains. The entity shall obtain approval of the data governance and management policies.	P1	• Documented and approved data governance and management policies for the 13 data governance and management domains. • Minutes of meeting of the entity's data governance committee providing approval on the data governance and management policies.
DG.3.2	The entity shall develop entity specific data governance and management processes in alignment with the 'National Data Governance and Management Policies'. The processes, at minimum, shall include the following: • Process participants. • Process step preconditions. • RACI matrix. • Process Key Performance Indicators. The entity shall obtain approval of the data governance and management processes.	P1	• Documented and approved data governance and management processes for the 13 data governance and management domains. • Minutes of meeting of the entity's data governance committee providing approval on the data governance and management processes.
DG.3.3	The approved data governance and management policies and processes shall be maintained and published on the internal portal of the entity.	P1	• Screenshot of the approved data governance and management policies and processes maintained within the internal portal of the entity.
DG.3.4	All changes to the data governance policies and processes shall be documented with clear indication of the approvals obtained.	P2	• Documented and approved changes to the data governance policies and processes. • Minutes of meeting of the entity's data governance committee providing approval on the updated data governance policies and processes.

DG.4 Data Governance Training and Awareness

Policy Number	Criteria	Priority	Evidence
DG.4.1	The entity shall assess the data governance awareness and skills of the stakeholders and map their skill levels. The results of the skill level mapping shall be used to develop the appropriate training sessions for the stakeholders.	P1	• Documented and approved data governance skill mapping report. • Minutes of meeting of the entity's data governance committee providing approval on the skill mapping report.
DG.4.2	Training and awareness plan shall be developed to increase the adoption of the National Data Governance and Management policies. The plan, at minimum, shall include the following: • Objectives of the training and awareness sessions. • Training and awareness session topics covering all the domains of 'National Data Governance Framework'. • Stakeholder groups intended for the training and awareness sessions. • Training schedule. The entity shall obtain approval of the training and awareness plan.	P1	• Documented and approved training and awareness plan. • Minutes of meeting of the entity's data governance committee providing approval on the training and awareness plan.
DG.4.3	A communication plan shall be established to communicate the updates on the data governance and management initiatives to the intended stakeholders. The communication plan, at minimum, shall include the following: • Stakeholder Impact Analysis • Stakeholder classification based on the impact analysis. • Objectives of the communication. • Communication messages. • List of intended stakeholders. • Channels of communication. • Frequency of communication. The entity shall obtain approval of the communication plan.	P1	• Documented and approved communication plan along with stakeholder impact analysis outlining the stakeholder classification. • Minutes of meeting of the entity's data governance committee providing approval on the communication plan.
DG.4.4	The entity shall periodically conduct training and awareness sessions for the intended stakeholders on the National Data Governance Framework guidelines	P1	• Documented training and awareness session invites along with the stakeholder participation list.
DG.4.5	The entity shall periodically review and update the training, awareness, and communication plan.	P2	• Documented report containing at minimum the date of review on the training, awareness and communication plans, the periodic review observations along with recommended and approved changes. • Minutes of meeting of the entity's data governance committee providing approval on the updated data governance communication plan.

DG.5 Data Governance Compliance Assessment Framework

Policy Number	Criteria	Priority	Evidence
DG.5.1	The entity shall document and report evidence corresponding to the compliance assessment criteria to MTCIT as per the requirements outlined in the 'National Data Governance and Management Compliance Assessment Model'.	P1	• Documented and approved compliance assessment checklist aligning to the 'National Data Governance and Management Compliance Assessment Model' • Minutes of meeting of the entity's data governance committee providing approval on the compliance assessment checklist along with the attached evidence
DG.5.2	The entity shall establish data governance compliance assessment framework in alignment with the 'National Data Governance and Management Compliance Assessment Model'. The framework shall include, at minimum the following: • Periodic processes for measuring compliance. • Activities needed to plan and perform compliance assessments. • Activities needed for reporting the results of a compliance assessment. • Activities needed to address and escalate cases of non-compliance.	P1	• Documented and approved compliance assessment checklist aligning to the 'National Data Governance and Management Compliance Assessment Model' • Minutes of meeting of the entity's data governance committee providing approval on the compliance assessment checklist along with the attached evidence

DG.6 Data Governance Performance Management

Policy Number	Criteria	Priority	Evidence
DG.6.1	The entity shall establish KPIs (Key Performance Indicators) to monitor its performance across all data governance and management domains. The KPIs, at minimum, shall include the following: • Indicator Name • Indicator Owner • Calculation equation • Data Sources for calculating the indicator • Measurement frequency • Baseline and target values	P1	• Documented and approved data governance and management KPIs. • Minutes of meeting of the entity's data governance committee providing approval on the KPIs to monitor performance across all data governance and management domains.
DG.6.2	The entity shall periodically monitor the KPIs to verify that the implemented data governance and management initiatives and projects achieve their target objectives and outcomes and report performance of the data governance and management domains to the data governance committee.	P2	• Periodic reports outlining the entity's performance across the data governance and management program KPIs (e.g., email to the data governance committee containing performance report of the data governance and management domains)

4.2 Data Catalog (DC)

DC.1 Data Dictionary

Policy Number	Criteria	Priority	Evidence
DC.1.1	The entity shall create an inventory of all its data assets and identify the critical data elements for cataloging.	P1	• Data asset inventory (in a spreadsheet or a data catalog automation tool). • List of critical data elements utilized within the entity's business processes (in a spreadsheet or a data catalog automation tool). • Evidence of approval by the data owners of the respective business units on the data asset inventory.
DC.1.2	A data dictionary shall be developed that serves as repository for the entity's technical metadata. The data dictionary, at minimum, shall include the following: • Data element name as per the naming convention standards issued by MTCIT. • Data element size. • Data element type. • Master data source for the data elements documenting the authoritative source including the application name, source module, source table name and source column name. • Physical database, table, column, and file names. • Access permissions. • Retention, backup, and recovery rules for the data element.	P2	• Documented data dictionary (in a spreadsheet or data catalog automation tool) that is certified by the Data Owners.
DC.1.3	The data dictionary shall be periodically reviewed and updated.	P3	• A register containing information of periodic review observations, the recommended and approved changes along with the version history or evidence showcasing the data dictionary log in the data catalog automation tool.
DC.1.4	The entity shall develop and obtain approval on the processes for creating and updating the data dictionary along with certifying the metadata.	P1	• (This shall be covered as part of the DG.3.2 criterion)
DC.1.5	An audit trail shall be maintained for viewing all updates made to the data dictionary.	P3	• Version history containing all updates made to the data dictionary along with the employee making the change or evidence of audit trail of the data dictionary within the data catalog automation tool.
DC.1.6	The data dictionary shall be stored in a central location along with appropriate access rights assigned to the relevant stakeholders.	P2	• Data dictionary storage location along with list of stakeholders, their roles and the level of access granted to the data dictionary or evidence showcasing access matrix of the data catalog automation tool.

DC.2 Business Glossary

Policy Number	Criteria	Priority	Evidence
DC.2.1	The entity shall develop a business glossary to establish and promote a common understanding of business terms used across its business processes. The business glossary, at minimum, shall include the following: • Name of the business term. • Definition of the business term. • Subject area classification (Finance, Human Resources, Procurement etc.) • Primary data classification (Top Secret, Secret, Restricted, Confidential, Unclassified) and supplementary markers of the business term • Ownership and stewardship for the business term. • Business rules associated with the business term. • Synonyms (or aliases) used for the business term. • Key Performance Indicators (KPIs), along with the calculation methodology	P1	• Documented business glossary (in a spreadsheet or a data catalog automation tool) that is certified by the Data Owners of the respective business units.
DC.2.2	The business glossary shall be periodically reviewed and updated.	P2	• A register containing information of periodic review observations, the recommended and approved changes along with the version history or evidence showcasing the business glossary log in the data catalog automation tool.
DC.2.3	The entity shall link the business glossary to its data dictionary.	P2	• A spreadsheet comprising officially certified data dictionary alongside its corresponding approved business glossary or evidence showcasing business glossary mapping with data dictionary in the data catalog automation tool.
DC.2.4	The entity shall develop and obtain approval on the processes for creating, updating, and certifying the business glossary.	P1	• (This shall be covered as part of the DG.3.2 criterion).
DC.2.5	An audit trail shall be maintained for viewing all updates made to the business glossary.	P3	• Version history containing all updates made to the business glossary along with the employee making the change or evidence of audit trail of the business glossary within the data catalog automation tool.
DC.2.6	The business glossary shall be maintained in a central location along with appropriate access rights assigned to the relevant stakeholders.	P1	• Business glossary storage location along with list of stakeholders, their roles and the level of access granted to the business glossary.

DC.3 Data Lineage

Policy Number	Criteria	Priority	Evidence
DC.3.1	The entity shall establish a data lineage to visually represent the movement and transformation logic of its metadata from source to target systems.	P2	• Documented data lineage showcasing the visual representation of source to target mapping or evidence showcasing source to target mapping within the data catalog automation tool.
DC.3.2	The entity shall develop and obtain approval on the processes for creating, updating, and certifying the data lineage.	P1	• Documented and approved processes for creating, updating, and certifying data lineage. • Minutes of meeting of the entity's data governance committee providing approval on the data lineage processes.
DC.3.3	An audit trail shall be maintained for viewing all updates made to the data lineage.	P3	• Version history containing all updates made to the data lineage along with the employee making the change in a spreadsheet or evidence of the audit trail of data lineage within the data catalog automation tool.
DC.3.4	The data lineage shall be stored in a central location along with appropriate access rights assigned to the relevant stakeholders.	P2	• Data lineage storage location along with list of stakeholders, their roles and the level of access granted to the data lineage or evidence showcasing access matrix of the data catalog automation tool.

DC.4 Data Catalog Automation Tool

Policy Number	Criteria	Priority	Evidence
DC.4.1	The entity shall onboard and adopt a data catalog automation tool for automating the creation, update and certification processes of the data dictionary, business glossary and data lineage.	P2	• Evidence of lineage diagram, business glossary definition and functional data dictionary on the data catalog automation tool.
DC.4.2	The data models related to the Data Catalog tool shall be aligned and ensured to be consistent with the enterprise data architecture.	P2	• Evidence of the data model of the Data Catalog tool aligning with the enterprise data architecture. (e.g., screenshot of the data model naming convention as per the naming convention standards defined in the enterprise data architecture)
DC.4.3	The entity shall develop a plan and obtain approval for connecting the data sources to the data catalog automation tool for onboarding the data dictionary and uploading the business glossary.	P2	• Documented and approved plan for implementing the data catalog automation tool containing the prioritization of data sources. • Minutes of meeting of the entity's data governance committee providing approval on the plan for connecting the data sources to the data catalog automation tool.
DC.4.4	Automated workflows shall be configured for data dictionary, business glossary and data lineage within the data catalog automation tool. The workflows, at minimum, shall include the following: • Creation and update of data dictionary along with certification of metadata. • Creation, update, and certification of business glossary. • Creation, update, and certification of data lineage. • Data Catalog access management.	P2	• Evidence of implemented workflows for data dictionary, business glossary and data lineage within the data catalog automation tool.

4.3 Data Classification (CL)

CL.1 Data Classification Impact Assessment

Sr. No.	Criteria	Priority	Evidence
CL.1.1	The entity shall prioritize its data assets to establish the order of classification.	P1	• Prioritized list of data assets for classification. • Approval from Data Owners of respective business units for the prioritized list of data assets (e.g., e-mail, minutes of meeting etc.).
CL.1.2	The data assets shall be classified into one of the primary data classification labels namely Top Secret, Secret, Restricted and Confidential as per the 'Royal Decree No. 118/2011- Issuing the Law Classifying the State's Documents and Regulating the Protected Places' or marked unclassified.	P1	• Documented data classification register. • Evidence demonstrating the approval of the data owner on the data classification labels assigned to the datasets of their respective business units.
CL.1.3	The entity shall establish and follow approved processes for assigning the appropriate primary data classification label to its data assets. The process at minimum, shall include the following activities: • Conduct impact assessment to identify the potential damage or impact that can be caused by the loss, misuse, or unauthorized disclosure of the data asset. The impact assessment shall at minimum cover the following dimensions: ○ Identification of potential impact arising from disclosure or unauthorized access to data. ○ Mapping of the identified potential impact to the business impact levels from 4 to 1. ○ Mapping of the data assets to the appropriate primary data classification labels namely Top Secret, Secret, Restricted, and Confidential as per the assessed business impact levels from 4 to 1 respectively. All data assets that are assessed to not fall under any of the primary data classification labels, shall be marked as 'Unclassified'	P1	• Documented data classification register including the potential impact of unauthorized disclosure, misuse, or loss of the data assets.
CL.1.4	The entity shall obtain approval on the assigned data classification labels of its data assets.	P1	• Documented data classification register. • Evidence demonstrating the approval of the data owner on the data classification labels assigned to the datasets of their respective business units.

CL.2 Supplementary Markers

Policy Number	Criteria	Priority	Evidence
CL.2.1	The entity shall define a list of entity specific supplementary markers (caveats and dissemination limiting markers) to be applied on top of the primary data classification labels to further limit the information dissemination as per its requirements.	P1	• Documented and approved list of supplementary markers of the entity. • Minutes of meeting of the entity's data governance committee providing approval on the supplementary markers.
CL.2.2	The entity shall evaluate and may apply one or more appropriate supplementary markers to its data assets that are classified as Top Secret, Secret, Restricted and Confidential to control the dissemination of data assets.	P1	• Documented and approved list of data assets tagged with one or more defined supplementary markers (e.g., spreadsheet, data catalog automation tool). • Approval from Data Owners of respective business units for the supplementary markers tagged to the data assets (e.g., e-mail, minutes of meeting etc.).
CL.2.3	The entity shall assess and mark its unclassified data assets with the supplementary marker 'FOR PUBLIC RELEASE' as per Article 28 of the 'National Data Strategy' for making them available as open data and contribute towards building a knowledge-based society. The assessment shall include at minimum the following: • Potential conflict with the existing laws/policies. • The benefits of applying the supplementary marker 'FOR PUBLIC RELEASE' vs. the negative impact. Please refer the National Data Governance and Management Policies document for details of the supplementary marking scheme.	P1	• Assessment report outlining: ○ Recommendations for tagging unclassified data assets with the supplementary marker "FOR PUBLIC RELEASE'. ○ Reasons for not tagging an unclassified data asset with the supplementary marker "FOR PUBLIC RELEASE'. • Approval from Data Owners of respective business units on the assessment Report.
CL.2.4	The supplementary markers for all the data assets shall be defined as metadata within the entity's business glossary as defined in the Data Catalog Policy.	P2	• Evidence of appropriate supplementary markers tagged to the data assets within the entity's business glossary (within a spreadsheet or data catalog tool) along with their approval (e.g., e-mail, Minutes of meeting)

CL.3 Data Classification Review

Policy Number	Criteria	Priority	Evidence
CL.3.1	The entity shall define the criteria that can trigger the declassification or downgrade of the classification labels for each of its data assets.	P1	• Defined and approved criteria for declassification and classification downgrade for each data asset. • Approval from Data Owners of respective business units for the declassification or downgrade to the classification labels. (e.g., e-mail, minutes of meeting etc.).
CL.3.2	The entity shall develop and follow a process for reviewing and updating the assigned data classification labels to its data assets. The process at minimum shall include the following activities: • Declassification or a downgrade of the data classification performed to reflect the change in the business impact levels of the data asset. • The receiving entity challenging the data classification assigned by an originating entity.	P1	• (This shall be covered as part of the DG.3.2 criterion).
CL.3.3	The data classification labels for all the data assets shall be defined as metadata within the entity's business glossary as defined in the Data Catalog Policy.	P2	• Data classification labels added as metadata within the entity's business glossary.

CL.4 Data Classification Artefacts

Policy Number	Criteria	Priority	Evidence
CL.4.1	The entity shall maintain a data classification register containing the assigned primary classification labels and supplementary markers to its data assets. The entity can leverage its data catalog automated tool for this purpose. The register, at minimum, shall include the following: • List of the entity's data assets. • Primary data classification labels and supplementary markers assigned to the data assets along with dates of assignment. • Duration for which the assigned security classification is valid. The duration of the data classification shall at maximum be the retention period defined for the data asset. • The declassification or downgrade triggers for the data asset as defined by the entity during the assignment of primary data classification labels. • A log of the data classification activities conducted on the data asset along with the details of primary classification labels and supplementary markers review.	P2	• The entity's data classification register (spreadsheet or data catalog).

4.4 Data Quality (DQ)

DQ.1 Data Quality Framework

Policy Number	Criteria	Priority	Evidence

DQ.1.1	The entity shall establish a data quality framework for operationalizing the entity specific data quality management initiatives. The framework, at minimum, shall include the following:
	• Identification of the data quality dimensions to address the data quality issues. The dimensions, at minimum, shall include one or more of the following:
	  ○ Completeness - Extent to which desired data is available for use.
	  ○ Consistency - Extent to which identical data has the same value across the systems.
	  ○ Accuracy - Extent to which data value matches with the real value.
	  ○ Timeliness - Extent to which the up-to-date data is available.
	  ○ Uniqueness - Extent to which unique data is available without duplication.
	• Approach for calculating the data quality scores. The data quality scoring approach, at minimum, shall include the following:
	  ○ Threshold percentage for each of the Data Quality Dimensions for meeting business expectations and the business impact of exceeding the threshold. For example: For assessing data quality completeness, metrics may include the percentage of missing values. A threshold of 4% or less indicates that the data is considered complete.
	  ○ Formula to calculate the data quality score.
	• Data quality index to showcase the change in the data quality score over a time period.
		P1	• Documented and approved data quality framework covering (at minimum) the data quality dimensions, approach for data quality scoring and data quality index.
			• Minutes of meeting of the entity's data governance committee providing approval on the data quality framework.

DQ.1.2	The entity shall develop and obtain approval on the process for monitoring and identifying the data quality issues.	P1	• (This shall be covered as part of the DG.3.2 criterion).
DQ.1.3	The entity shall define and obtain approval on the process for remediating the data quality issues. The process, at minimum, shall include the following: • Root cause analysis to identify the cause of the issue. • Remediation options to address the root cause. • Plan to implement the selected remediation option. • Implementation and validation of the selected remediation option.	P1	• (This shall be covered as part of the DG.3.2 criterion).
DQ.1.4	The entity shall develop and obtain approval for data quality Service Level Agreements (SLAs) which, at minimum, shall include the following: • Timeline for developing plans to fix data quality issues. • Timeline for implementing and reviewing data quality changes. • Escalation actions for SLA violations.	P1	• Documented and approved Service Level Agreements (SLAs) for data quality covering implementation timelines along with escalation actions. • Minutes of meeting of the entity's data governance committee providing approval on the data quality Service Level Agreements (SLAs).

DQ.2 Data Quality Operations

Policy Number	Criteria	Priority	Evidence
DQ.2.1	The entity shall develop and document the data quality rules for the business-critical data elements based on the data quality dimensions.	P1	• Documented and approved data quality rules for business-critical data elements. • Evidence of the approval provided by the data owners on the data quality rules (For e.g., minutes of meeting, emails).
DQ.2.2	The entity shall conduct data quality profiling as per the data quality execution plan to monitor the data quality health.	P1	• Documented data quality profiling result. • Email demonstrating the regular distribution of data quality profiling reports to the stakeholders.
DQ.2.3	The entity shall evaluate the data profiling result to analyze the requirement of rule change or threshold reconfiguration to refine the data quality monitoring inputs.	P1	• Documented and approved actions based on the data quality profiling results. • Minutes of meeting of the entity's data governance committee providing approval on the actions based on the data quality profiling results.
DQ.2.4	The entity shall conduct root cause analysis for the identified data quality issues and prepare data quality remediation report. The report shall include, at minimum the following: • Description of the data quality issues. • Impact of the data quality issues (business unit level/ entity level). • Root cause analysis results of the identified issues. • Recommended activities for issue resolution.	P1	• Documented and approved data quality remediation report. • Evidence of the approval provided by the data owners on the data quality remediation report (For e.g., minutes of meeting, emails).
DQ.2.5	Data quality remediation plan shall be developed by the entity to implement the activities recommended for the resolution of the issues. The plan, at minimum, shall include the timeline and milestones for implementation of the recommended activities. The entity shall obtain approval on the developed data quality remediation plan.	P1	• Documented and approved data quality remediation plan. • Evidence demonstrating the approval of the data owner on the data quality remediation plan (For e.g., minutes of meeting, emails).
DQ.2.6	The data quality issue remediation shall be monitored as per the entity's data quality Service Level Agreements.	P2	• A report containing the actual timelines of remediating data quality issues vs the defined SLAs. • Evidence of review by Data Owners on the report (e.g., DQ remediation status meetings with attendance of Data Owners, screenshots of automated dashboards published to Data Owners along with walkthrough of workflows etc.)
DQ.2.7	The entity shall maintain a data quality issues log. The log shall include, at minimum the following: • Data quality issue description. • Corrective or Preventive actions performed on the issue. • Degree of data quality improvement. • Number of data quality issues resolved vs the number of data quality issues identified. • Number of SLA breaches	P2	• Documented data quality issue log. • Evidence of review by Data Owners on the data quality issue log. (e.g., Minutes of meeting with attendance from the Data Owners etc.).

DQ.3 Data Quality Automation Tool

Policy Number	Criteria	Priority	Evidence
DQ.3.1	The entity shall onboard and adopt a tool for implementing the processes of data quality management within the tool as automated workflows. The workflows at minimum shall include the following: • Workflows for automated discovery of data quality issues as per the data quality rules defined across the data quality dimensions. • Workflow for automated routing of the identified data quality issues to the relevant stakeholders. • Workflows for generating standardized reports and dashboards summarizing key data quality metrics and trends within the entity data.	P2	• Data Quality profiling results/dashboard within the data quality automation tool. • Evidence of functional data quality workflows on the data quality automation tool.

4.5Data Operations (DO)

DO.1 Data Storage

Policy Number	Criteria	Priority	Evidence
DO.1.1	The entity shall conduct periodic storage infrastructure utilization forecast of its information systems based on the future business requirements. The forecast, at minimum, shall include the following: • Storage capacity needs as per the planned application initiatives • Estimated budget for the future storage requirements	P1	• A register/report documenting the periodic storage infrastructure utilization forecasts along with the approvals obtained on them. • Minutes of meeting of the entity's data governance committee providing approval on the infrastructure utilization forecast.
DO.1.2	The entity shall define a process and obtain approval for evaluating and selecting the database technology. The evaluation, at minimum, shall include the following: • Total ownership cost. • Data volume capacity of the technology. • Security controls provided by technology. • Availability of skilled resources within and outside of the entity.	P1	• Documented and approved process for database technology selection. • Minutes of meeting of the entity's data governance committee providing approval on the process for selecting database technology.
DO.1.3	The entity shall define and obtain approval for the process of using digital means for data collection and shall maintain a register to document the reason for not collecting data through a digital means.	P1	• (This shall be covered as part of the DG.3.2 criterion).
DO.1.4	The entity shall define and obtain approval for the process of providing role-based access to the relevant employees and contractors to the entity's database. Access controls for employees and contractors of the entity shall be determined by their respective classification labels, which are based on the nature of their work performed within and for the entity	P1	• (This shall be covered as part of the DG.3.2 criterion).
DO.1.5	The entity shall regularly monitor and report the performance of the database.	P2	• Documented report for database performance monitoring along with details of review and approval. • Evidence of the entity's IT Head providing approval on the database performance monitoring report (e.g., email, minutes of meeting where the approval was provided etc.)
DO.1.6	The entity shall define and obtain approval on the Service Level Agreements of database performance requirements, data availability and recovery requirements.	P2	• Documented Service Level Agreements (SLAs) as per the requirements for database performance and recovery. • Minutes of meeting of the entity's data governance committee providing approval on the SLAs.
DO.1.7	The entity shall define and implement the retention periods for data based on business, regulatory and legal requirements.	P2	• Documented and approved retention periods for entity's critical data assets. • Evidence showcasing the approval of the data owner on the retention periods of critical data (For e.g., minutes of meeting, emails)
DO.1.8	The entity shall conduct periodic reviews and update the defined retention periods as per requirements.	P3	• A register containing information of periodic review observation, the recommended approved changes along with version history. • Email/screenshot of the approval from the Data Owner of the respective business unit on the register containing information of periodic review observation.
DO.1.9	The entity shall define and implement archival period of the data as per the business and regulatory requirements.	P2	• Documented and approved archival periods for entity's data assets. • Evidence showcasing the approval of the data owner on the archival periods of data assets (For e.g., minutes of meeting, emails).
DO.1.10	The entity shall define and obtain approval on the rules for disposal of the data based on the classification levels and tables of common and specific retention periods approved for each entity.	P1	• Documented data disposal rules of the data assets mapped to the data classification. • Evidence showcasing the approval of the data owner on the rules for disposal of the data assets (For e.g., minutes of meeting, emails).
DO.1.11	The entity shall document a list of safe destruction methods and obtain approval to implement it on the archived data.	P1	• Documented and approved destruction methods for the entity's data assets. • Evidence showcasing the approval of the data owner on the list of safe destruction methods for disposing

Policy Number	Criteria	Priority	Evidence
			entity's data assets (For e.g., minutes of meeting, emails).

DO.2 Backup and Restore

Policy Number	Criteria	Priority	Evidence
DO.2.1	The entity shall establish and follow a process for data backup and restore. The process, at minimum, shall include the following: • Backup frequency for each information system. • Backup scope of each information system along with the data range. • Backup location along with the storage medium. • Backup validation. • Restore through change request.	P1	• (This shall be covered as part of the DG.3.2 criterion).
DO.2.2	The entity shall conduct periodic recovery testing to ensure successful restoration of the backup within a timeframe.	P2	• Documented outcomes from the periodic recovery tests including the target v/s actual recovery time periods. • Evidence of the entity's Database Administrator providing approval on the periodic recovery tests (e.g., email, minutes of meeting where the approval was provided etc.)
DO.2.3	The entity shall verify the validity of the restored data before transferring it to the production environment.	P2	• Checklist containing the acceptance criteria to validate the restored data. • Evidence of the entity's Database Administrator providing sign-off on the performed validation testing as per the acceptance criteria.

DO.3 Disaster Recovery

Policy Number	Criteria	Priority	Evidence
DO.3.1	The entity shall develop and obtain approval on the disaster recovery plan to ensure limited-service disruption in case of prolonged system outage.	P2	• Documented and approved disaster recovery plan. • Minutes of meeting of the entity's data governance committee providing approval on the disaster recovery plan.
DO.3.2	The entity shall develop a list of information systems ranked based on their business criticality and potential monetary and reputational losses because of emergency or disaster. The list of systems, at minimum, shall include the following: • Recovery Time Objective – Maximum permissible outage time of the information system without causing business damage. • Recovery Point Objective – Maximum permissible data the entity can afford losing without causing business damage.	P2	• Documented and approved list of information systems ranked as per order of recovery in case of an emergency or disaster. • Defined and approved Recovery Time Objective and Recovery Point Objective for each information system. • Minutes of meeting of the entity's data governance committee providing approval on the Recovery Time Objective and Recovery Point Objective.
DO.3.3	In the event of permanent loss of large volume of highly valued data (Data Classified as Top Secret and Secret), the entity shall develop a data loss case report. The data loss case report, at minimum shall include the following: • Lost data description • Criticality of the data • Data loss cause • Date and time of data loss	P2	• Documented and approved data loss case report. (For e.g., report, template). • Minutes of meeting of the entity's data governance committee providing approval on the data loss case reporting template. • Documented details of data loss in the event of permanent loss of Top Secret and Secret Classification data signed off by the entity's data governance committee (e.g., minutes of meeting providing the sign-off).
DO.3.4	The entity shall draft a report on the data loss incident, outlining lessons learned and preventive measures. The report shall then be submitted to the data governance committee for approval and direction.	P2	• Documented and approved preventive measures against the data loss cases. • Minutes of meeting of the entity's data governance committee providing approval and directions on the data loss incident report.

4.6 Data Architecture (DA)

DA.1 Data Architecture

Policy Number	Criteria	Priority	Evidence
DA.1.1	The entity shall develop and document its current state data architecture for outlining the existing structure, components and processes involved in managing and utilizing its data from source to the target applications. The current state data architecture, at minimum, shall include the following: • Identification of data sources. • Identification of processes involved in existing business operations. • Data storage systems, data processing systems and data analytics platforms involved in the existing processes. • Data Architecture patterns in terms of data ingestion and provisioning as per the existing processes. The entity shall obtain approval on the current state data architecture.	P1	• Documented and approved current state data architecture. • Minutes of the meeting of the DG Committee providing approval on the current state data architecture.
DA.1.2	The business and technical requirements shall be identified and documented as per the entity's planned data initiatives. The requirements, at minimum, shall include the following: • The data required along with their sources as per the purpose and scope of the data initiative. • Requirements of the data platform in terms of data ingestion, storage, data processing and provisioning as per the objectives of the data initiative.	P1	• Documented list of business and technical requirements for entity's target state data architecture.
DA.1.3	The entity shall review its current state data architecture and develop its target state data architecture as per the activities identified to address the gaps. The target state architecture shall be developed in alignment with the overall enterprise architecture standards. The target state data architecture, at minimum, shall include the following: • Identification of data sources. • Identification of processes involved as per the planned data initiatives. • Data storage systems, data processing systems and data analytics platforms involved in the business processes of the planned data initiatives. • Data Architecture patterns in terms of data ingestion and provisioning as per the existing processes. The target state data architecture shall be reviewed to ensure that it addresses the requirements of the entity's planned data initiatives. Additionally, the entity shall obtain approval on the target state data architecture.	P2	• Documented and approved target state data architecture. • Minutes of meeting of the entity's data governance committee providing approval on the target state data architecture.
DA.1.4	The entity shall establish data architecture checkpoints within its software development lifecycle to review and assess impact on its data architecture due to any system development initiative.	P2	• Documented architecture compliance review process along with roles and responsibilities.
DA.1.5	The data architecture shall be monitored and updated in case of any changes to the entity's data systems which include the following cases: • Change in the structure of the existing data within the systems. • Changing the data integration methods for accessing or sharing data from multiple systems. • Changing the data sources or data storage systems.	P3	• Target state data architecture version history consisting of the changes made, the change requests received that triggered the change along with the approving authority name and designation.
DA.1.6	The entity shall define and obtain approval on the process to update and receive approval for any updates made to the data architecture. The process, at minimum, shall have the following steps: • Reviewing the data architecture change request. • Conducting impact assessment to identify the affected architecture components. • Updating the impacted architecture components. • Obtaining approval, updating the data architecture, and publishing it. The entity shall obtain approval on the process for its implementation	P2	• Documented and approved data architecture change management process. • Minutes of meeting of the entity's data governance committee providing approval on the data architecture change management process.
DA.1.7	The entity shall adopt a suitable tool to design and maintain its data architecture. The tool, at minimum, shall support the following capabilities: • Data Architecture design. • Impact analysis to analyze the risk of changes to the data architecture components.	P2	• Document providing evidence of a functional data architecture design tool (e.g. - Screenshot of the enterprise data architecture within the data architecture tool).
DA.1.8	The data architecture shall be stored in a central location with appropriate access rights assigned to the relevant stakeholders.	P2	• Data architecture storage location along with list of stakeholders, their roles and the level of access granted to the data architecture.
DA.1.9	All updates made to the data architecture shall be tracked through a version control mechanism.	P3	• Version history containing all updates made to the data architecture along with the employee's name a designation making the changes or evidence of the audit trail within the data architecture tool.

DA.2 Data Models

Policy Number	Criteria	Priority	Evidence
DA.2.1	The entities shall develop and document data models to define the structures and relationships of the data within its system components The data models, at minimum, shall include the following: • The conceptual data model showcasing the involved data entities, their attributes and relationship between the data entities. • The logical data model based on the conceptual data model along with the data constraints. • The physical data model based on the logical data model and including the table and column level information for each of the data entities. The entity shall obtain approval on the developed and documented data models	P2	• Documented and approved data models including the conceptual, logical, and physical data models. • Evidence showcasing approval from the Enterprise Data Architect on the data models (For e.g., email or minutes of meetings).
DA.2.2	The entity shall define the naming convention standards to be used for developing the data models. The naming convention standards shall be documented as technical metadata within the entity's data dictionary as per its Data Catalog Policy.	P1	• Documented and approved naming convention standards for enterprise data architecture. • Minutes of meeting of the DG Committee providing approval on the naming convention standards for enterprise data architecture. • Screenshot of the entity's data dictionary showcasing the naming convention standards as technical metadata.
DA.2.3	The entity shall establish a diagramming method to develop its data models.	P1	• Documented and approved diagramming method for data modeling. • Minutes of meeting of the DG Committee providing approval on the diagramming method data modeling.
DA.2.4	The entity shall establish checkpoints within its software development lifecycle to review and assess impact on its data models due to any system development initiative.	P1	• Documented data model compliance review process along with roles and responsibilities. • Evidence of review (e.g., impact assessment report) and approval by the enterprise data architect (e.g. email, minutes of meeting providing the approval) on the impact to the entity's data models due to any system development initiative.
DA.2.5	The entity shall adopt a suitable tool to design and maintain its data models. The tool, at minimum, shall support the following capabilities: • Graphical representation of the data model. • Automated redrawing of relationships based on movement of entities.	P2	• Evidence demonstrating the implementation of a data modeling tool (e.g.- screenshot of the defined data models within the data modeling tool).
DA.2.6	The data models shall be monitored and updated in case of any changes to the entity's data systems which include the following cases: • Change in the structure of the existing data within the systems. • Changing the data sources or data storage systems.	P3	• Version history containing all updates made to the data models along with the employee's name and designation making the change or evidence of the audit trail within the data model tool.
DA.2.7	A entity shall obtain approval on a process to update and receive approval for any changes made to the data models. The process shall at minimum include the following steps: • Reviewing the data model change request. • Conducting impact assessment to identify the affected data model components. • Updating the impacted data model components • Obtaining approval, updating the data architecture, and publishing it	P2	• Documented and approved process for data model change management. • Minutes of meeting of the entity's data governance committee providing approval on the data model change management process.
DA.2.8	The data models shall be stored in a central location with appropriate access rights assigned to the relevant stakeholders.	P2	• Data models storage location along with list of stakeholders, their roles and the level of access granted to the data models.
DA.2.9	All updates made to the data models shall be tracked through a version control mechanism.	P3	• Version history containing all updates made to the data models along with the employee's name and designation making the change or evidence of the audit trail within the data model tool.

4.7 Data Sharing and Integration Policy (DSI)

DSI.1 Data Sharing Methods

Policy Number	Criteria	Priority	Evidence
DSI.1.1	The entity shall detail the functional and non-functional requirements into an integration requirements document as per its planned and approved data analytics business cases and obtain approval on the integration requirement document. The requirements, at minimum, shall include the following: • The purpose and scope of the use case for data collection/sharing. • Data availability requirements (e.g., real-time, near real time, batch etc.). • Regulatory requirements, if any, governing the collection, storage, retention and archival of data. • Implementation Timeline • Cost Estimate	P1	• Integration requirements document covering the minimum functional and non- functional requirements. • Evidence showcasing the approval of the data owner on the integration requirements document (For e.g., minutes of meeting, emails).
DSI.1.2	The entity shall assess its current integration architecture to identify the gaps with respect to the data integration requirements.	P1	• Current integration assessment report. • Evidence showcasing approval from the Enterprise Data Architect on the current integration architecture report (For e.g. email or minutes of meetings).
DSI.1.3	A target integration architecture shall be created to bridge the identified gaps. The target integration architecture, at minimum, shall include the following: • The data sources, intermediary systems, and data platforms along with target systems (internal/external). • Data Integration patterns (ETL – Extract transform and load, ELT – Extract load and transform, event streaming, API - Application Programming Interface and data virtualization) as per the data availability requirements. • Technical standards for data and information exchange outlined in the "Systems Integration Policy for Government Entities – Published by MTCIT."	P2	• Documented and approved target integration architecture • Minutes of meeting of the Data Governance Committee providing the approval on the target integration architecture.
DSI.1.4	The entity shall develop a solution integration design as per its target integration architecture. The solution integration design, at minimum, shall include the following: • Overview of the integration solution supported by the solution overview diagram. • Data flow diagram representing the flow of data between the systems sharing data. • Mapping specifications for all the intermediary staging areas where the data is being transformed between the source and the target systems. • Security requirements to be considered.	P2	• Documented and approved solution architecture design • Minutes of meeting of the Data Governance Committee providing the approval on the solution architecture design.
DSI.1.5	The entity shall test the developed integration solution prior to its deployment to the production environment to verify its alignment to the solution integration design. The testing, at minimum, shall consist of the following: • **Integration testing:** verifying the correctness of data flows between integrated technology components (systems, applications, data stores) to identify and resolve any data quality issues. • **Functional testing:** verifying that the system meets both functional and non-functional requirements and satisfies purpose of the data collection/sharing. Each of the above shall, at minimum, include the following: • Defining the test cases. • Setting up the test environment • Executing the test cases in a test environment and documenting test results	P2	• Documented test cases for validating the integration solution including the results of the testing. • Evidence of approval by the enterprise data architect on the test execution results (e.g., Minutes of meeting providing the approval, email etc.)
DSI.1.6	The entity shall monitor and maintain the solution integration design to incorporate any changes in the integration requirements. The monitoring and maintenance, at minimum, shall include the following: • Reporting on any identified issues • Documenting change requests on the integration requirements from the end users.	P2	• Solution integration design issue register. • Solution integration design change request register.

DSI.2 Data Sharing Agreements

Policy Number	Criteria	Priority	Evidence
DSI.2.1	The entity shall develop and obtain approval on a Data Sharing Agreement Template for creating a contractual agreement with parties for internal (in case the data providers and consumers are from different departments) and external data sharing. The template, at minimum, shall include the following fields: • Purpose of the data sharing request. • Legal basis (statute or royal decree) for data sharing request (e.g., statute, royal decree allowing the entity to share data or signed agreements) • Declaration of the technical and security measures available at the requestor's end for ensuring data protection • Minimum volume of data required to achieve the purpose of the data sharing request. • Requirements for data to be shared namely, data format, data accuracy, level of detail, data structure, data type, masking, anonymization (in case of Personally Identifiable Information (PII) data) and aggregation. • Liability Provisions in case of non-compliance with the provisions of the data sharing agreement. • Restrictions on data usage and sharing with third parties	P1	• Documented and approved internal and external data sharing agreement templates. • Minutes of meeting of the DG Committee providing approval on the data sharing agreement template.
DSI.2.2	The entity shall ensure that it is the producer of the data requested for sharing to establish that the data is being requested from the right source.	P1	• Documented list of data assets being shared along with their data sources and the department within the entity owning the data source.
DSI.2.3	The entity receiving the data shall comply with the data classification level stipulated by the originating entity.	P1	• Classification of the data asset as per the Data Sharing Agreement. • Evidence Classification of the data asset as per the entity's data catalog/business glossary.
DSI.2.4	The entity shall ensure that data is appropriately classified among Top Secret, Secret, Restricted, Confidential, Unclassified before sharing it internally or externally.	P2	• Documented and approved data classification label of the data asset being shared. (For e.g., Data Classification Labels of the data assets documented in the Data Classification Register). • Evidence showcasing approval of the data owners on the classification label of data assets of their business unit being shared (For e.g. minutes of meeting, emails)
DSI.2.5	The data sharing agreement shall include a clause that prohibits data requestors from making copies of shared data or sharing the data received without the consent of the producer of the data. Exceptions (if any) shall be explicitly mentioned in the data sharing agreement.	P1	• Documented and approved data sharing agreement template with the clause and provision for exceptions. • Minutes of meeting of the DG Committee providing approval on the internal and external data sharing agreement templates.
DSI.2.6	The data sharing agreement shall be signed by the relevant executives before data is shared.	P2	• Documented data sharing agreements signed by the relevant executives involved in data sharing. • Signed data sharing agreement by the data owner authoring the sharing of data of their business unit.
DSI.2.7	The entity shall give priority to approved and secure sharing media for exchanging data.	P2	• Evidence of usage of the data integration platform or Government Unified Portal (GUP) for data exchange (e.g., defined, and approved solution integration design showcasing integration with the data integration platform or GUP)
DSI.2.8	In case of sharing of personal data, the identity of the data subjects shall be anonymized, unless the identity is necessary for the purpose of sharing. Necessary controls shall be maintained to protect the privacy of the data subjects in accordance with the 'Personal Data Protection Policy'	P2	• Evidence of anonymization, masking, encryption while sharing of personal data. • Evidence showcasing approval of the data owners on the implemented security protocols (anonymization, masking, encryption) while sharing personal data (For e.g. minutes of meeting, emails)
DSI.2.9	A process shall be developed and followed as per the SLA stipulated in the National Data Strategy for the assessment and fulfillment/rejection of the external data sharing requests. The entity sharing the data may stipulate the conditions for agreeing to the data sharing request such as the data retention rules for the data being shared etc.	P1	• (This shall be covered as part of the DG.3.2 criterion).

Policy Number	Criteria	Priority	Evidence
DSI.2.10	A record of data sharing requests received, and the decisions made against them shall be developed and maintained.	P1	• A register containing details of data sharing requests and decisions made against them. • Evidence showcasing approval of the data owners on the data sharing register.
DSI.2.11	The entity shall periodically review and update the data sharing agreements to incorporate any changes in the contractual requirements.	P2	• A register containing details of reviews conducted on the data sharing agreements along with the incorporated changes.
DSI.2.12	A mechanism shall be created and followed for receiving and routing the internal and external data sharing requests to the appropriate roles as per the responsibilities outlined in the 'Data Governance and Management Office Establishment Guidelines'.	P1	• Documented mechanism for routing of data sharing requests. • Minutes of meeting of the DG Committee providing approval on the mechanism for receiving and routing the internal and external data sharing requests.

DSI.3 Data Sharing Automation Tool

Policy Number	Criteria	Priority	Evidence
DSI.3.1	The entity shall evaluate and adopt a tool as per its solution integration design to automate the internal and external data sharing as workflows. The workflows at minimum, shall include the following: • Assessment and fulfillment/rejection of the data sharing requests as per pre-defined rules. • Automated routing of the data sharing requests to the appropriate roles. • Data sharing tool access management.	P2	• Document providing evidence of a functional data exchange automation tool with 54minimum workflows.

4.8 Data Analytics (AN)

AN.1 Business Cases

Policy Number	Criteria	Priority	Evidence
AN.1.1	The entity shall identify and create an exhaustive list of its analytics business cases (including potential business cases for advanced analytics) across the entity's business functions. The business case definition shall at minimum include the name, description and the business functions involved in implementing the business cases.	P1	• Documented exhaustive list of business cases for analytics implementation. • Evidence showcasing the approval of the data owner on the exhaustive list of business cases. (For e.g., minutes of meeting, emails).
AN.1.2	A business case prioritization matrix shall be created to prioritize the exhaustive list of analytics business cases. The matrix shall at minimum have the following criteria: • Alignment to the business objectives of the entity. • Feasibility of implementation • Financial impact due to implementation • Business benefits due to implementation including the targeted Return on Investment (ROI) • Technical complexity of implementing the business case.	P1	• Documented and approved business case prioritization matrix. • Minutes of meeting of the entity's data governance committee providing approval on the business case prioritization matrix.
AN.1.3	The business cases shall be shortlisted based on their feasibility and validity as determined from the technical complexity (including the needed tools), required skillset etc. The entity shall obtain approval on the shortlisted business cases for their implementation.	P1	• Documented and approved shortlist of business cases for analytics implementation. • Minutes of meeting of the entity's data governance committee providing approval on the analytics business cases for implementation.
AN.1.4	The exhaustive list of analytics business cases shall be periodically reviewed and updated.	P2	• Documented updated list of business cases for analytics implementation along with evidence of periodic review. For e.g., minutes of meeting of the analytics ideation sessions.

AN.2 Data Analytics Implementation

Policy Number	Criteria	Priority	Evidence
AN.2.1	The entity shall document the requirements for the approved business cases. The requirements, at minimum, shall include the following: • The objective of the business case. • The required data and its sources. • The required quality of data. • The expected business value through the development of the business case. • The type of analytics (prescriptive, descriptive, diagnostic, predictive) to be utilized. • Performance, usability, and workflow requirements. • Technologies required for implementing the business case including the Data storage, processing, and integration requirements. • Criteria for successful implementation of the business case.	P1	• Documented functional and technical requirements for approved business cases. • Evidence showcasing the approval of the data owner on the business case requirements. (For e.g., minutes of meeting, emails).
AN.2.2	The entity shall develop a plan and obtain approval for implementing the approved analytics business cases The plan shall at minimum, include the following activities: • Detailing the functional and non-functional requirements for translating the business case objectives into analytics requirements including the scope and acceptance criteria. • High-level conceptual design of the analytics solution e.g., wireframes • The environments (e.g., Dev, QA, UAT and production) for hosting the analytics solution during and after the development. • Developing the functional and non-functional requirements to meet the high-level conceptual design. • Testing the developed solution as per the defined scope and acceptance criteria. • Deployment timeline/schedule for establishing a pilot and/ or delivery of the business case. • Required personnel within the entity that possess the necessary skills to execute the business case. • Availability and quality of the required data. • The data management activities (acquisition, integration, quality check, enrichment, storage, processing etc.) required to deliver the analytics business case.	P1	• Documented and approved analytics business case implementation plan. • Minutes of meeting of the entity's data governance committee providing approval on the analytics business cases implementation plan.
AN.2.3	The entity shall implement and validate the outcomes of the implemented analytics business cases. The validation activities shall at minimum, include the following: • Functional and non-functional requirements • Personal Data Protection considerations • Validation of business impact including the ROI as per the target set.	P2	• Documented test case results of analytics business case implementation. • Evidence of the periodic review results for the implemented analytics business cases (e.g., report for notifying the senior executives on the periodic validation of the analytics business cases)
AN.2.4	The outcomes shall be documented, and the benefits delivered shall be socialized to all the relevant stakeholders.	P2	• Documented impact and benefits to the business operations due to the implementation of analytics business cases • Evidence of communicating the impact/ benefits to relevant stakeholders (e.g., email to the relevant stakeholders outlining the benefits delivered through implementation of analytics business case.)

AN.3 Data Analytics Tools

Policy Number	Criteria	Priority	Evidence
AN.3.1	The entities shall adopt and onboard a data analytics tool for automated insight generation and reporting. The features of the tool, at minimum, shall include the following: • Automated visualization and reporting of metrics as per defined frequency. • Support integration with a variety of data sources. The data sources, at minimum, shall include databases, data warehouses, data lakes, cloud storage, data streams and files. • Capability to support creation of workflows for data collection, transformation and enrichment, analysis and reporting to enable collaboration among the data analytics roles.	P2	• Evidence demonstrating the implementation of data analytics tool (e.g.- Screenshot of automated visualization and reporting metrics in the data analytics tool.)

AN.4 Data Platforms

Policy Number	Criteria	Priority	Evidence
AN.4.1	The entity shall onboard and adopt data platforms that support implementation of advanced analytics initiatives. The platforms, at minimum, shall support the following features: • Integration with various data sources namely, databases, data warehouses, data lakes, data lakehouses, cloud storage, data streams and files. • Data profiling and remediation workflows to handle missing values along with identification of the data quality dimensions • Data enrichment capabilities through integration with third-party tools. • Capabilities for advanced statistical analysis namely, regression, clustering, time series analysis and predictive modeling. • Self-service reporting that enables users to create custom reports as per requirements. • Capability to handle large data volumes along with high performance ability. • Capability to support creation of workflows for data collection, transformation and enrichment, analysis and reporting to enable collaboration among the data analytics roles.	P2	• Evidence demonstrating the implementation of data platform, for example – evidence showcasing data profiling and remediation workflows to handle missing values along with identification of the data quality dimensions within the data platform.

4.9 Open Data (OD)

OD.1 Open Data Identification

Policy Number	Criteria	Priority	Evidence
OD.1.1	The entity shall identify all its "Unclassified" data assets marked 'FOR PUBLIC RELEASE' as Open Data, in alignment with its data classification policy and the Article 28 of the 'National Data Strategy'.	P1	• Documented list of open data assets
OD.1.2	A process for identification of Open Data assets from among the inventory of data assets shall be developed and followed by the entities. The process, at minimum, shall include the following steps: • Prioritization of the data assets as per their importance to be published as open data. • Identification of data sources for the data assets including the associated metadata. The entity's data catalog may be leveraged for this purpose. • Impact assessment on the data assets (along with related metadata) for identifying their potential to be classified as public data. • Evaluating alignment of the open data assets with the outlined policy principles. • Certification of the identified open data assets. The entity shall obtain approval on the process for identifying its open data assets	P1	• (This shall be covered as part of the DG.3.2 criterion).
OD.1.3	A list of all the identified and certified open data assets shall be created. The list, at minimum, shall have the following information: • Name of the open data asset. • The data sources for the open data asset • Log of open data publishing and modification activities on the corresponding open data assets. • The executive role within the entity responsible for certifying the open data.	P1	• Documented and approved list of open data assets with the minimum attributes. • Evidence showcasing certification of the identified open data assets by the Data Owners of the respective Business Units.

OD.2 Open Data Publishing

Policy Number	Criteria	Priority	Evidence
OD.2.1	The government entity shall publish all its specified open data assets on the National Open Data Portal in accordance with the specifications outlined in the Open Government License.	P2	• Documented log of open data assets of the entity. • Links to the documented open data assets from the entity's official website.
OD.2.2	The entity shall develop a standard structure for publishing its open data assets. The structure, at minimum, shall have the following attributes: • Name of the open data asset. • Descriptive information necessary to describe the open data for the understanding of the public. • Department responsible for the open data. • The date on which the open data asset was last reviewed and updated.	P1	• Documented and approved structure for publishing open data assets. • Minutes of meeting of the entity's data governance committee providing approval on the analytics business cases implementation plan.
OD.2.3	The entity shall develop a register of the open data that is published. The register shall at minimum include the following information: • Name of the open data asset. • Information about the open data asset i.e., metadata, includes: Dataset Title, Data Description, Category Name, Keywords, Publication Date, Modification Date, Contact Point Name and Address, File Format, Publication Frequency, and Language. • Additionally, include variable descriptions such as: Variable Name, Variable Description, Data Type (Date, Text, and Numeric), Obligation Level (Mandatory, Optional). • Name of the person or Department responsible for the data asset within the government entity. • Format of the published data asset (XML, JSON, XLS, CSV) • Schedule for updating the data asset.	P2	• Developed and approved register of the published open data assets. • Evidence of approval by the data owners on the register of the published open data assets (e.g., e-mail approval, minutes of meeting providing the approval)
OD.2.4	The entity shall periodically evaluate the possibility of f marking data as 'Unclassified' to make additional data available for public release as open data.	P2	• Documented and approved log of data assets that are unclassified and marked with the supplementary marker 'FOR PUBLIC RELEASE' along with their original classification and date of publishing as open data. • Evidence of approval received from the Data Governance Committee (e.g. e-mail approval, minutes of meeting of the Data Governance Committee).
OD.2.5	A process shall be developed for assessing and responding to the public requests received from the National Open Data Portal for sharing additional open data assets. The process, at minimum, shall include the following steps: • Receipt and acknowledgement of the open data sharing request. • Communication of the assessment outcome (accepted/rejected) to the requestor along with justification within 15 working days. • Making the requested additional open data available to the requestor in case the request is accepted.	P2	• Documented and approved process for handling public requests for additional open data assets. • Evidence of approval received from the Data Governance Committee (e.g. e-mail approval, minutes of meeting of the Data Governance Committee).
OD.2.6	Open data assets shall be published by adhering to the standard formats consistent with the principles of open data policy.	P2	• Links to the published open data assets.
OD.2.7	Periodic review and maintenance of the published open data assets shall be carried out by the entities to ensure adherence to the relevant regulatory requirements.	P3	• Log of reviews conducted on the published open data assets along with the incorporated changes.
OD.2.8	An automated tool shall be leveraged by the entities to implement the processes of open data identification and publishing as automated workflows.	P3	• Evidence of automated open data publishing process showcasing workflows for open data identification and publishing within the tool.

4.10 Reference and Master Data (RMD)

RMD.1 Reference Data Management

Policy Number	Criteria	Priority	Evidence
RMD.1.1	The entity shall identify and create a list of reference data objects that are utilized within its business processes based on the analysis of the data catalog and existing data models.	P2	• Documented list of identified reference data objects. • Evidence of approval from Data Owners of the respective business units on the identified reference data objects (e.g., emails, minutes of meeting providing details of approval).
RMD.1.2	The entity shall review its existing information system landscape and identify the systems where the reference data objects are read.	P2	• Documented list of source systems for reference data objects. • Evidence of approval from enterprise data architect on the identified list of source systems for reference data objects (e.g., emails, minutes of meeting providing details of approval).
RMD.1.3	Processes for creating, updating, and deleting/archiving the reference data shall be developed and followed. The entity shall obtain approval on the processes for their implementation.	P2	• Documented and approved processes for creating, updating, and deleting/archiving reference data across the entity. • Evidence of approval from the Data Governance Committee (e.g. emails, Minutes of meeting providing the details of approval).
RMD.1.4	Ownership and stewardship roles shall be assigned to the relevant stakeholders for managing the reference data within the entity.	P2	• Documented and approved roles and responsibilities for managing reference data aligning to the 'Data Governance and Management Office Establishment Guidelines'. • Mapping of the ownership and stewardship roles to the relevant employees of the entity. • Evidence of the approval from the Data Governance Committee (e.g. emails, Minutes of meeting providing the details of approval).
RMD.1.5	The reference data shall be added as metadata within the entity's business glossary.	P2	• Business glossary including identification of reference data objects. • Evidence of certification of the reference data objects as part of the business glossary.
RMD.1.6	The entity shall periodically review and update the list of reference data objects as per their usage status within the entity's business processes.	P3	• Log of reviews conducted on the list of reference data objects along with the incorporated changes.
RMD.1.7	The entity shall maintain a version control to ensure traceability of all the updates made to the list of reference data objects.	P3	• Version history containing all updates made to the reference data objects list along with the employee's name and designation making the change.

RMD.2 Master Data Management

Policy Number	Criteria	Priority	Evidence
RMD.1.1	The entity shall identify and create a list of master data objects that are utilized within its business processes based on the analysis of the data catalog and existing data models.	P2	• Documented list of identified master data objects. • Evidence of approval from Data Owners of the respective business units on the identified reference data objects (e.g., emails, minutes of meeting providing details of approval)
RMD.1.2	The entity shall review its existing information system landscape and identify the systems where the master data objects are created, read, updated, or deleted.	P2	• Documented list of source systems for master data objects. • Evidence of approval from enterprise data architect on the identified list of source systems of the master data objects (e.g., emails, minutes of meeting providing details of approval).
RMD.1.3	Processes for creating, updating, and deleting/archiving the master data shall be developed and followed. The entity shall obtain approval on the processes for their implementation.	P2	• Documented and approved processes for creating, updating, and deleting/archiving master data across the entity. • Evidence of the approval from the Data Governance Committee (e.g. emails, Minutes of meeting providing the details of approval).
RMD.1.4	Ownership and stewardship roles shall be assigned to the relevant stakeholders for managing the master data within the entity.	P2	• Documented and approved roles for managing master data and their responsibilities aligning to the 'Data Governance and Management Office Establishment Guidelines'. • Mapping of the ownership and stewardship roles to the relevant employees of the entity. • Evidence of the approval from the Data Governance Committee (e.g. emails, Minutes of meeting providing the details of approval).
RMD.1.5	The master data shall be defined as a metadata attribute within the entity's business glossary.	P2	• Business glossary including identification of master data objects. • Evidence of certification of the master data objects as part of the business glossary.
RMD.1.6	The entity shall periodically review and update the list of master data objects as per their usage status within the entity's business processes.	P3	• Documented updated list of master data objects.
RMD.1.7	The entity shall maintain a version control to ensure traceability of all the updates made to the list of master data objects.	P3	• Documented version control logs containing all update activities for master data objects.

RMD.3 Reference and Master Data Automation Tool

Policy Number	Criteria	Priority	Evidence
RMD.3.1	The entity shall identify the requirements for creating and provisioning the authoritative data to the target systems. The requirements, at minimum, shall include the following: • Data sources to be integrated. • Target systems consuming the authoritative data. • Data quality rules to be enforced. • The required integration and orchestration patterns.	P3	• Documented and approved reference and master data requirements document. • Evidence of approval from Data Owners of the respective business units on the requirements for creating and provisioning the authoritative data (e.g., emails, minutes of meeting providing details of the approval).
RMD.3.2	The entity shall, based on its requirements, evaluate, and select a suitable reference architecture pattern from among Consolidation, Registry and Coexistence architecture patterns for designing the Reference and Master Data hub (RMD hub).	P3	• Documented reference and master data architecture pattern. • Evidence of the approval from the Data Governance Committee (e.g., emails, Minutes of meeting providing the details of approval).
RMD.3.3	The entity shall design a solution architecture based on the reference architecture pattern selected. The solution architecture, at minimum, shall include the following: • The Create, Read, Update, and Delete (CRUD) matrix for defining the master data sources. • Master data records between the data sources and the RMD hub. • Authoritative records between the data hub and target systems. • Reference data between data hub and consuming applications. • The conceptual, logical, and physical data models including hierarchy and relationships between the master data tables reference and Master Data hub (RMD hub). List of reference data tables. • The data dictionary containing the description of the master data elements along with the source to target transformation logics and Delete (CRUD) matrix for defining the master data sources.	P3	• Documented and approved reference and master data solution architecture design. • Evidence of the approval from the Data Governance Committee (e.g., emails, Minutes of meeting providing the details of approval).
RMD.3.4	The entity shall evaluate and onboard a reference and master data automation tool to implement the solution architecture design and provide authoritative records to the target systems. The tool implementation, at minimum, shall include the following requirements: • Data quality rules to be enforced to ensure data accuracy and up to date data • Technical and security controls to monitor the access to the authoritative data	P3	• Evidence demonstrating the implementation of master data management tool, for example data validation, data quality rules within the automated tool.
RMD.3.5	A version control shall be implemented in the tool for maintaining an audit trail of all the updates made to the reference and master data records.	P3	• Evidence of audit trail feature within the implemented reference and master data automation tool.

4.11 Data Monetization (DM)

DM.1 Revenue Streams Creation

Policy Number	Criteria	Priority	Evidence
DM.1.1	The entity shall conduct a data monetization opportunity assessment to identify and document an exhaustive list of data products for revenue streams creation by leveraging its data.	P2	• Documented list of data products for revenue generation across the entity. • Minutes of meeting of the data monetization opportunity assessment workshop/meeting, containing agenda, discussion points and outcomes along with the attendees.
DM.1.2	Business cases shall be developed for the identified data products. The business case, at a minimum, shall include the following: • Targeted segment/s and market size. • Benchmarking analysis on the associated trends. • Estimated costs and revenue. The entity shall obtain approval on the business cases for implementation.	P2	• Documented and approved business cases for the identified data products. • Minutes of meeting of the entity's data governance committee providing approval on the revenue streams creation business cases.
DM.1.3	The entity shall develop data product designs for the approved business cases. The data product designs, at minimum, shall include the following: • Functional and non-functional requirements. • Data and technical architecture of the data products. • Data product business model including identification of the targeted customers, partnership for development of data product, data product sale model (subscription based, freemium, one-time payment etc.)	P2	• Data product designs for the approved business cases. • Evidence of approval by the enterprise data architect on the data product designs (e.g., minutes of meeting where the approval has been provided, email etc.)
DM.1.4	The entity shall determine the price for each of the designed data products. The price of the data products shall only be charged from non-government entities that are using the data products. The following, at minimum, shall be considered for determining the product price: • Expected demand for the data product. • Benchmark price as per the market analysis. • Expected cost. The entity shall get the pricing model reviewed and obtain approval for its implementation.	P2	• Documented product price against each of the designed data products. • Minutes of meeting of the entity's data governance committee providing approval on pricing of the data product.
DM.1.5	A financial plan shall be developed for estimating the commercial feasibility of developing and operationalizing the data product. The plan, at minimum, shall include the following: • Addressable market size • Expected revenue. • Return on Investment (ROI) and Payback period. The entity shall get the financial plan reviewed and obtain approval for its implementation.	P2	• Documented and approved financial plan for the designed data products. • Minutes of meeting of the entity's data governance committee providing approval on financial plan of the data product.
DM.1.6	The entity shall define a charging model for each of the shortlisted data products intended to generate revenue. The charging models shall be selected from the following: • Consumption-based model: Charging dependent on consumer's usage of data products. • Freemium/premium model: Offering basic features free and charging for the premium features. • Subscription model: Charging based on monthly recurring fees. • One-time free model: Charging one-time fee from consumers for the data products. The entity shall get the charging model reviewed and obtain approval for its implementation.	P2	• Documented and approved charging model for the shortlisted data products. • Minutes of meeting of the entity's data governance committee providing approval on charging model of the data product.
DM.1.7	The implemented data products shall be periodically monitored and enhanced to achieve the required ROI within the calculated payback period.	P3	• Documented and approved outcomes from monitoring the implemented data products.

DM.2 Cost Optimization

Policy Number	Criteria	Priority	Evidence
DM.2.1	The entity shall identify the opportunities to leverage its data to streamline its operations across business units. For example: • Automating workflows to limit repetitive operations and avoiding errors. • Optimizing service delivery, reducing bottlenecks, and enhancing citizens satisfaction.	P2	• Documented and approved opportunities for streamlining operations across entity's business units. • Minutes of meeting of the entity's data governance committee providing approval on opportunities to leverage data for streamlining entity's operations.
DM.2.2	The entity shall leverage its data to identify opportunities for enhancing its strategic decision making. For e • Optimizing resource allocation across operations • Energy consumption optimization in public places • Optimizing procurement and contract costs • Route optimization and fleet management for public transportation	P2	• Documented and approved opportunities for enhancing strategic decision making across entity's business units. • Minutes of meeting of the entity's data governance committee providing approval on opportunities to leverage data for enhancing entity' decision making.
DM.2.3	The outcomes from the implementation of the identified opportunities shall be periodically monitored and enhanced.	P3	• Documented outcomes from monitoring the implemented opportunities.

4.12 Freedom of Information (FOI)

FOI.1 Information Request Management

Policy Number	Criteria	Priority	Evidence
FOI.1.1	The entity shall develop and obtain approval for the process of managing the request to access entity's unpublished official information.	P2	• Documented and approved processes for managing the request to access entity's unpublished official information. • Minutes of meeting of the entity's data governance committee providing approval on the processes for managing the request to access entity's unpublished official information.
FOI.1.2	The entity shall establish methods including both paper-based and electronic formats, for requesting access to or obtaining unpublished official information.	P3	• Paper-based and electronic based information request forms.
FOI.1.3	Identity of the individuals shall be verified before granting access to the requested unpublished official information.	P3	• Evidence showcasing verification of the individual's identity for granting access to the requested unpublished information.
FOI.1.4	The entity shall make the information request forms available on its official website, for requesting access to the entity specific unpublished official information. The request form, at minimum, shall include the following: • Name of the requestor • Civil Identification Number of the Requestor. • Contact information of the requestor. • Purpose of the information request.	P3	• Link to the information request form on the official website.
FOI.1.5	The entity shall review the requested information within a month of its receipt and notify its decision to either approve, deny, or intimate an extended timeline for the response. The entity shall obtain approval on the notification before being sent to the requestor.	P3	• Documented response to the requested information along with the request receipt date. • Evidence of approval by the Data Governance and Management Head on the response (e.g., E-mail, Minutes of meeting providing the approval etc.)
FOI.1.6	Charges for processing information requests, shall be standardized.	P3	• Documented and approved pricing scheme for requests to access entity's unpublished official information. • Evidence of approval from the Data Governance Committee on the pricing scheme (e.g., E-mail, Minutes of the meeting providing the approval etc.)
FOI.1.7	In case of denial of a request, the requestor shall be notified of the reasons for denial along with instructions to initiate grievance, if any.	P3	• Documented responses along with appropriate reasoning for all denied requests. • Evidence of approval by the Data Governance and Management Head on the response (e.g., E-mail, Minutes of meeting providing the approval etc.)
FOI.1.8	The entity shall ensure a balance between right to access information and considerations such as national security and the protection of personal data while responding to public requests for accessing unpublished official information.	P3	• A documented and approved report detailing assessment of the information request with respect to national security and personal data protection considerations. • Evidence of approval by the Data Governance and Management Head on the assessment report (e.g., E-mail, Minutes of meeting providing the approval etc.)

FOI.2 Issue and Grievance Management

Policy Number	Criteria	Priority	Evidence
FOI.2.1	The entity shall develop a process for handling the issues and grievances raised by the requestor based on the received information. The process shall include an activity to review the decisions on issues and grievances by the data governance committee to ensure they are transparent, and free from undue influence or bias.	P3	• Documented and approved process for grievance handling. • Evidence of approval from the Data Governance Committee on the grievance handling process (e.g., E-mail, Minutes of the meeting providing the approval etc.)
FOI.2.2	Decisions on issue and grievance shall be communicated to the requestor in writing, providing reasons for the decision and information on further recourse, if available.	P3	• Documented and approved decisions on the information request. • Minutes of meeting of the entity's data governance committee providing approval on the information request decisions.
FOI.2.3	The entity shall maintain a register to document the information requests along with the corresponding information or responses shared.	P3	• Documented FOI register containing all information requests along with corresponding responses.

4.13 Personal Data Protection Policy (PDP)

PDP.1 Controlling Entity Obligations

Policy Number	Criteria	Priority	Evidence
PDP.1.1	The controlling entity shall commit to protect all the information and personal data in its possession, including the information and data received from other units, or those that have been disclosed to other units.	P1	• Evidence of the controls implemented to protect the personal data (e.g., screenshot of consent forms, screenshots of privacy notice displayed, evidence showcasing implementation of security protocols such as masking, anonymization, encryption before sharing personal data etc.) • Evidence of approval by the Information Security Officer on the controls implemented to protect personal data.
PDP.1.2	When processing personal data, the controlling entity shall at minimum consider the following: • The Data is collected through legitimate and fair means and that the collection is limited to what is necessary to meet its legal requirements or related to its direct business activity. • Data processing is fair and lawful. • Data is true and accurate and is updated when necessary. • Data does not remain in a form that allows the data subject to be identified after the purpose for which it was collected or for which subsequent processing is carried out has been exhausted.	P1	• Documented and approved consent form or screenshot of the electronic consent form(s) and privacy notice related to a particular business process. • Evidence showcasing the approval of the Data Protection Officer on the consent form(s) and privacy notice.
PDP.1.3	The controlling entity shall request to obtain minimum amount of data and documents from the data subject to complete service transactions, in the event that they are not available electronically or are not available for electronic circulation with any other government unit.	P1	• Documented and approved personal data processing register containing purposes and the minimum required personal data. • Record of personal data collected corresponding to the minimum required personal data for each service transaction within the personal data processing register. • Evidence showcasing the approval of the Data Protection Officer on the personal data processing register (e.g. email, minutes of meeting etc.).
PDP.1.4	The controlling entity shall implement security and organizational measures to protect data from accidental or unauthorized destruction or accidental loss, or from unauthorized alteration, disclosure, hacking, or any other form of processing.	P1	• Documented and approved preventive measures to protect personal data. (For e.g., implementation of access control measures as per data classification). • Vulnerability assessment and recommended security measures report approved by the Information Security Officer.

Policy Number	Criteria	Priority	Evidence
PDP.1.5	The controlling entity shall establish adequate security precautions for all systems and storage media involved in dealing with data to prevent any type of hacking.	P1	• Evidence of the controls implemented to protect the personal data (e.g., encryption, masking, anonymization etc.) • Evidence of approval by the Information Security Officer on the controls implemented to protect personal data.
PDP.1.6	In case where the processing unit or any third party assigned to process personal data, the controlling unit shall at minimum ensure the following: • The processing unit/third party provides adequate guarantees regarding the application of the technical and organizational measures that must be considered when processing data and takes the necessary steps to verify compliance with them. • The processing shall be carried out in accordance with a written contract concluded between the controller and the processing unit/third party that processes the data on its behalf or under its supervision. • Clear stipulations are included in the contract regarding retention periods and arrangements for deleting data sent or received.	P1	• Defined and signed personal data processing contract (physical /electronic) with clear stipulations on the personal data processing, retention periods and disposal rules. • Defined and signed personal data processing contract (physical /electronic) with clear agreement on the technical and organizational measures taken by the third party processing unit. • Evidence showcasing personal data processing contract signed by the data protection officer (e.g., email, digital signature, physical signature etc.).
PDP.1.7	The controlling unit shall disclose acquired or updated data with the third-party processing unit - as long as there is a clear and valid purpose for the disclosure in accordance with legal obligations and privacy considerations.	P1	• Defined and signed personal data processing contract outlining the legal statute/obligation for disclosure of personal data to the third-party processing unit. • Evidence showcasing personal data processing contract signed by the data protection officer (e.g., email, digital signature, physical signature etc.).
PDP.1.8	The controlling entity shall display a privacy notice on its website to provide the data subjects with information on their personal data collection, its processing. The privacy statement shall at minimum include the following: • The purpose of collecting data. • Whether collecting all or some of it is mandatory or optional. • Information to the data subjects that their personal data will not be processed in a way that is inconsistent to the purpose of collecting it. • The types of personal data that will be collected. • The means used to collect, process, store and dispose the personal data. • The unit or units to which the personal data will be disclosed, its description, and whether the personal data will be transferred, disclosed, or processed outside the Sultanate. • Potential consequences and risks of not completing the personal data collection procedure of the entity.	P2	• Link of the privacy notice on entity's website outlining the privacy notice informing the data subjects of their rights over their personal data collected by the entities.
PDP.1.9	The privacy notice shall inform the data subjects of their rights over their personal data collected by the entities. The following rights shall be included in the privacy notice: • The right to information, including being informed of the purpose of collecting data. • The right to access their personal their personal data available to the controlling entity in accordance with the relevant regulations and policies. • The right to request access to their personal data available to the controlling entity in a legible and clear format. • The right to request the correction, completion or updating of personal data available to the controlling entity.	P2	• Link to the privacy notice on the entity's website, offering comprehensive information to data subjects regarding their rights pertaining to the collection of their personal data by the entity.
PDP.1.10	The controlling entity shall establish mechanisms to ensure the safe destruction of personal data in order to prevent unauthorized parties from accessing the data.	P1	• Documented and approved rules for disposal of the personal data. • Evidence showcasing the approval of the Data Owner on the personal data disposal rules (e.g., email)
PDP.1.11	The controlling entity shall notify the Electronic Defense Center in the event of any leakage, damage or hacking of personal data.	P1	• Documented and approved mechanism to notify the Electronic Defense Center in the event of a leak, damage to, or hacking of personal data. • Evidence showcasing the approval of the Data Protection Officer on the mechanisms to notify the Electronic Defense Center in the event of data leak, damage, hack etc.

Policy Number	Criteria	Priority	Evidence
PDP.1.12	The controlling entity shall process the personal data within the geographical borders of the Sultanate to ensure national sovereignty over personal data and the protection of privacy of the data subjects. Exceptions to the transfer or processing of personal data if any, shall be only for the following cases: • Execution of a contract outside the geographical borders of Oman to which the data subject is a party. • Initiating procedures to claim or defend legal rights. • Protecting the vital interests of the data subject.	P2	• Documented and approved register/ screenshot from data catalog automation tool containing details of the location and information systems where personal data is being stored and processed. • Evidence showcasing the approval of the Data Protection Officer on the register containing details of the location and information systems where personal data is being stored and processed.
PDP.1.13	The controlling entity shall obtain the approval of the Electronic Defense Center before transferring personal data outside the geographical borders of the Sultanate for the purpose of processing it.	P1	• Documented approval from the Electronic Defense Center for transferring personal data outside geographical borders.

PDP.2 Third Party Processing Unit Obligations

Policy Number	Criteria	Priority	Evidence
PDP.2.1	The third-party processing unit shall at minimum, commit to the following: • Protecting all the information and personal data in its possession, including information and data received from other units, or those that have been disclosed to other units. • The processing unit or third party shall not undertake any processing except in accordance with the instructions of the controlling entity.	P2	• Documented and signed contract between data controller and third party for processing the personal data.