



SDAIA
الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority

National Data Index

Document Classification: **Public**

Version 1.1

November 2024



Document Control

Version	Revision Date	Contributor	Modification
1.0	Oct 2023	SDAIA	First Draft
1.1	Nov 2024	SDAIA	Document Update

Table of Content

1. Document Objective	3
2. Table of Abbreviations.....	3
3. Introduction.....	4
4. NDI Overview.....	5
5. Scope.....	6
6. The NDI Framework.....	7
6.1. Benchmarking	8
6.2. Index Design.....	8
6.3. Outcomes	11
7. Summary	15
8. Appendix.....	15
8.1. Appendix I – DM Practices Maturity Assessment Questionnaire	15
8.2. Appendix II – Acceptance Evidence Checklists	87
8.3. Appendix III – Operational Excellence (OE)	246

1. Document Objective

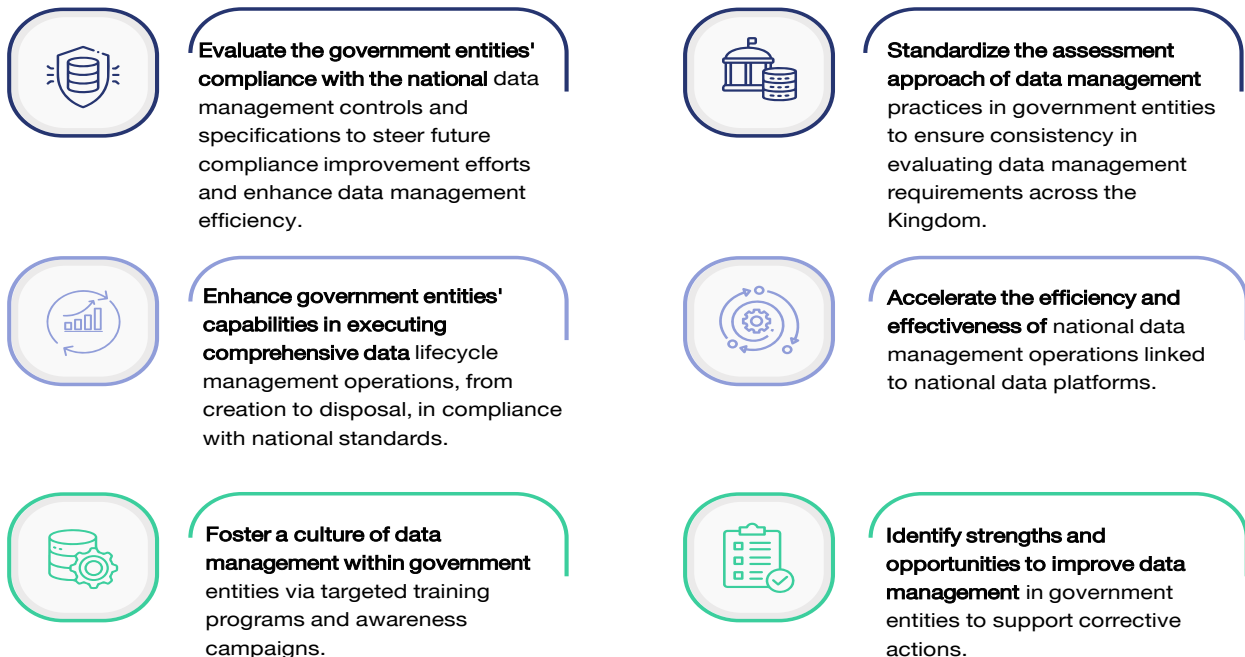
This document aims to present introductory details about the National Data Index (NDI). It includes the NDI's overview, scope, aims, framework, and components with their measurement scores and assessment levels which are described in the appendix.

2. Table of Abbreviations

Abbreviation	Definition
NDL	National Data Lake (A National Data Platform).
DM	Data Management.
DMP	Data Marketplace (A National Data Platform).
DG	Data Governance.
DQ	Data Quality.
GSB	Government Service Bus (A National Data Platform).
KSA	Kingdom of Saudi Arabia.
NDC	National Data Catalog (A National Data Platform).
NDI	National Data Index.
NDMO	National Data Management Office.
PDPL	Personal Data Protection Law
ODP	Open Data Platform (A National Data Platform).
OE	Operational Excellence.
PDP	Personal Data Protection.
RDP	Reference Data Management Platform (A National Data Platform).
SDAIA	Saudi Data and Artificial Intelligence Authority.

3. Introduction

The **Saudi Data & AI Authority (SDAIA)** is on the mission of developing a data-driven economy and fostering the Kingdom's data-literacy level to benefit from data for operational efficiency and insightful decision-making. From this perspective, SDAIA launched, as part of its initiatives, the National Data Index (NDI), which is a dynamic and result-oriented monitoring and evaluation index established to assess the productivity and track the progress of government entities with regards to the Maturity of the Data Management (DM) practices, Compliance to Data Management and Personal Data Protection (DM and PDP) Standards, and Operational Excellence (OE). The NDI is built to satisfy the data ecosystem requirements of the Kingdom of Saudi Arabia (KSA) specifically. This comprehensive framework serves as a reliable metric and an influential indicator, aiding the realization of Vision 2030's objectives by contributing to becoming a smart nation and building a thriving economy, a vibrant society, and an ambitious nation. The NDI provides government entities with the enablers that help effectively in measuring current DM practices and achieving high assessment levels, and aims high to achieve the following key objectives:





4. NDI Overview

SDAIA designed a specialized data index based on benchmark studies of global data indices to reach best practices. For activating the NDI, it is developed based on the following three components:

- **DM Practices Maturity Assessment:** Measuring the extent to which a government entity applies best practices in 14 DM domains related to people, technologies, and operational processes. Then, provide recommendations based on the results to improve the maturity levels of data management within government entity.
- **DM and PDP Standards Compliance Assessment:** Measuring the extent to which an entity adheres to the **Data Management and Personal Data Protection (DM and PDP) Standards** published by the **National Data Management Office (NDMO)**.
- **Operational Excellence (OE) Assessment:** Measuring the progress made in a government entity's operations in national data management across 6 data management areas through national data platforms.

The above NDI components will be measured and audited periodically using the NDI platform, which is the technological infrastructure of the assessments. The key NDI platform functionalities include:

- **Assessment Execution:** The NDI platform facilitates the automated execution of the measurements, ensuring standardized and efficient evaluation processes.
- **Data Analysis:** The NDI platform provides detailed reports on the results of the NDI components in an interactive and smooth manner.

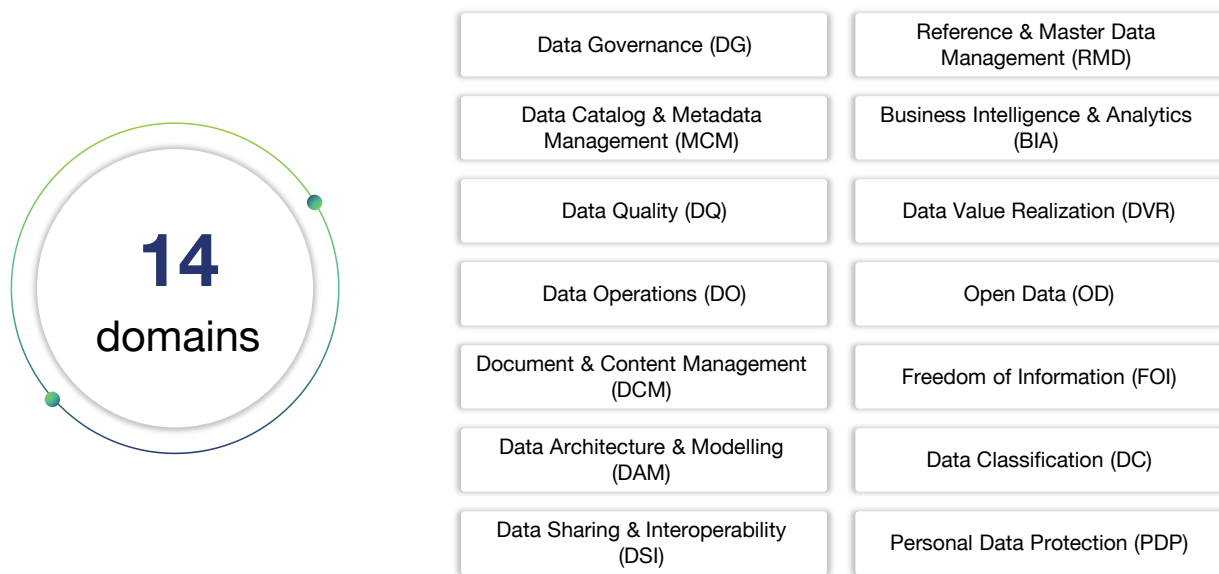
The NDI platform is a tool designed to facilitate the NDI assessment for the entity. Furthermore, it covers a range of functionalities that provide real-time capabilities, enabling the entity to closely track its incremental progress towards attaining a high NDI score.

5. Scope

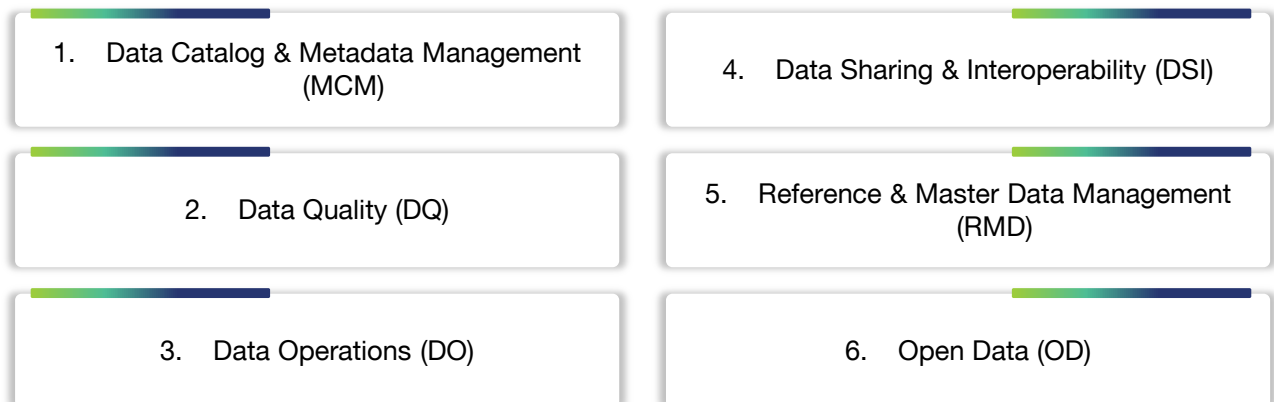


The NDI's scope of work represents practical auditing procedures to ensure accuracy in DM practices, integrity, and conformity of the targeted entities. NDI covers the following components and DM Domains:

For the Maturity and Compliance components, the NDI scope covers the following 14 DM domains:



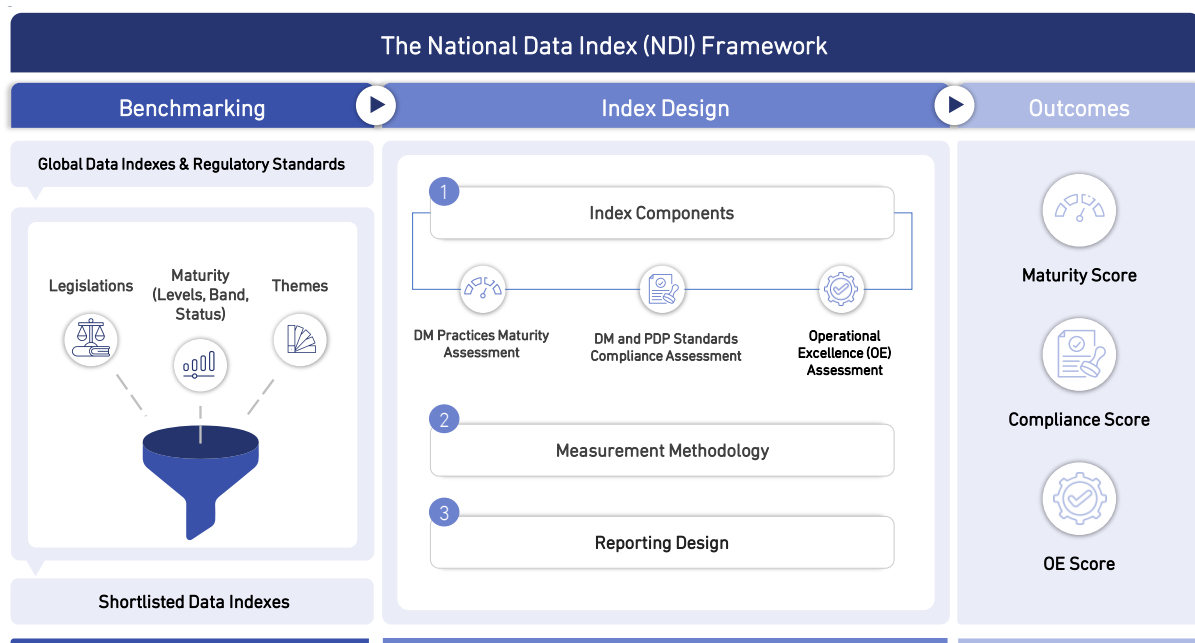
For the OE component, the NDI scope covers the following 6 prioritized DM Domains, as others shall be added gradually based on readiness:



This comprehensive approach enhances the empowerment of government entities, mainly in relation to data-based initiatives, by supporting a culture of continuous improvement, risk mitigation, and effective Data Governance. The NDI framework helps in providing the correct understanding of the strengths and gap fulfilments to improve the DM practices and maximize the value of the data assets.

6. The NDI Framework

The NDI Framework includes the index components, measurement methodologies, reporting, audits and governance mechanisms as shown in the figure below:



The NDI Framework is based on a systematic approach and methodology consisting of the following focal elements:



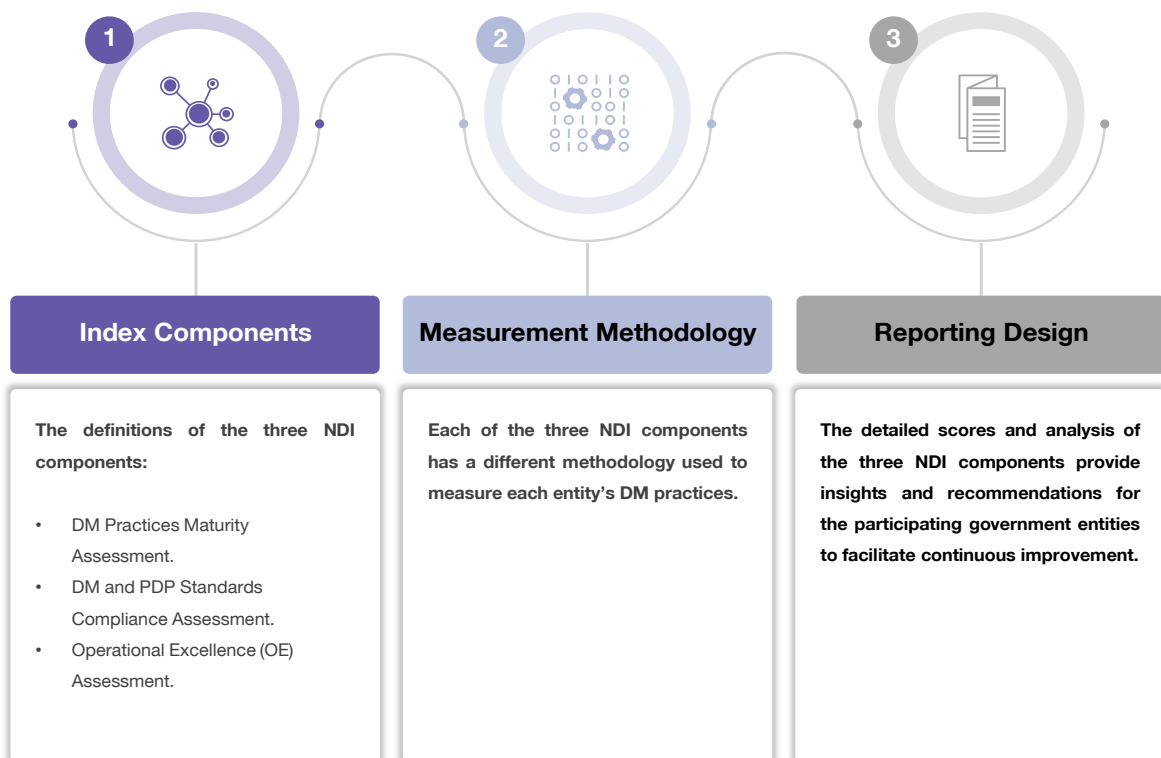
6.1. Benchmarking

Benchmarking was a strategic process followed to take into consideration the lessons learnt from global indices. The benchmarking outputs made SDAIA gain valuable ideas about the relative ranking of the methodologies and process efficiencies of these international data-related economic factors. This comparative analysis served as a crucial starting point for identifying the best practices that are implemented worldwide in data indices. Benchmarking was built on various sources such as: industry reports, surveys, case studies, best practices, themes, dimensions, etc. which were used to design the NDI.

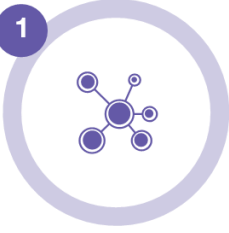


6.2. Index Design

The design of the NDI covers the various DM dimensions in alignment with the “DM and PDP Standards”, thus providing a progress roadmap for each government entity. As shown in the figure below, the NDI was designed by performing several activities, mainly: determining its components, formulating its measurement methodology, and designing its reporting mechanism:



1



The Index Components

The NDI has three components which are defined in the figure below and described in detail in the appendix. They will be measured through a comprehensive evaluation of each entity's Data Management practices. The NDI components are:

DM Practices Maturity Assessment

- This component measures the entities' maturity in Data Management (DM).
- It's shared with the entities which will participate in the NDI measurement to answer the questions and provide supporting evidences.
- It's managed through a dedicated measurement platform.
- It covers **14** DM domains published by the National Data Management Office (NDMO).
- The **14** DM domains have scoring weights assigned by SDAIA.



The DM and PDP Standards Compliance Assessment

- This component measures the Entities' Compliance with the **191** Specifications in the DM & PDP Standards published by the NDMO, all of which were mapped in the Maturity Questionnaire.
- The Compliance assessment results are obtained by answering the DM Maturity Questionnaire and completing the acceptance evidences.
- It covers **14** DM domains published by the NDMO.
- The **14** DM domains have scoring weights assigned by SDAIA.



The Operational Excellence (OE) Assessment

- This component measures the progress of entities' processes operationally which are based on the national platforms / technological solutions such as NDC, GSB, etc.
- It currently covers **6** of the DM domains published by NDMO.



2



The Measurement Methodology

It is developed for each NDI component, as each one has a different calculation and a separate result used for measuring its level for each entity:

- **The Maturity Assessment:** Is calculated using the Maturity questionnaire to measure the entity's maturity in 14 of the DM domains.
- **The Compliance Assessment:** The Compliance score is deduced from the entity's answers to the Maturity questionnaire, as the result shows the extent of the entity's commitment to implementing the 191 specifications of the DM domains published by the National Data Management Office (NDMO), namely, "Data Management and Personal Data Protection (DM and PDP) Standards".
- **The Operational Excellence (OE) Assessment:** Is applicable on 6 of the DM domains. It measures how progressive the entity is in terms of its DM operational processes by maximizing the benefit from the National Data Platforms, such as:
 - National Data Lake (NDL).
 - Data Marketplace (DMP).
 - National Data Catalog (NDC).
 - Government Service Bus (GSB).
 - Reference Data Management platform (RDP).
 - Open Data Platform (ODP).

3



Reporting Design

A special mechanism has been designed to generate the NDI reports, which present detailed results for each of the index components, and thorough details which allow the entity to understand its strengths, advancement opportunities, and areas of continuous improvement in its DM practices.



6.3. Outcomes

Based on the approved design of the NDI above, the NDI outcomes generate for each entity three scores which are described below:

The Score of the DM Practices
Maturity Assessment.



The Score of DM and PDP
Standards Compliance
Assessment



The Score of the Operational
Excellence (OE) Assessment





6.3.1. The Score of DM Maturity Practices Assessment

The DM Maturity Assessment contains 42 questions aimed at evaluating entities' Data Management practices across 14 DM domains. The Maturity assessment has 6 levels, ranging from **Level 0 “Absence of Capabilities”** to **Level 5 “Pioneer”**. The entity's overall maturity level for its DM practices shall be specified based on the percentage scale as described in the diagram below:

	0	1	2	3	4	5
Maturity Level	Absence of Capabilities	Establishing	Defined	Activated	Managed	Pioneer
Maturity Score Band	0 – 0.24	0.25 – 1.24	1.25 – 2.49	2.5 – 3.99	4 – 4.74	4.75 – 5
Maturity Percentage Scale	0%- 4.9%	5%- 24.9%	25%- 49.9%	50%- 79.9%	80%- 94.9%	95%- 100%
Maturity Level Description	Lack of fundamental data management capabilities, with no established practices.	Basic data management practices are introduced, but they are not standardized.	Data management practices have been developed and formalized, ensuring consistency and reliability.	Institutional processes, scalable tools and initial stages of automation have been implemented to support data management.	Centralized governance with end-to-end Key Performance Indicators (KPIs) and metrics are in place.	Continuous improvement is enabled, with a strong focus on data innovation and a reputation as a benchmark for excellence in data management
Maturity Question Coverage	No Practices	Identification	Development	Implementation or Execution	KPIs and Metrics	Continuous improvement
Objective	None	Building awareness	Developing best practice capabilities	Implementing and standardizing the developed practices	Managing practices and measuring progress	Innovation



6.3.2.The Score of the DM and PDP Standards Compliance Assessment

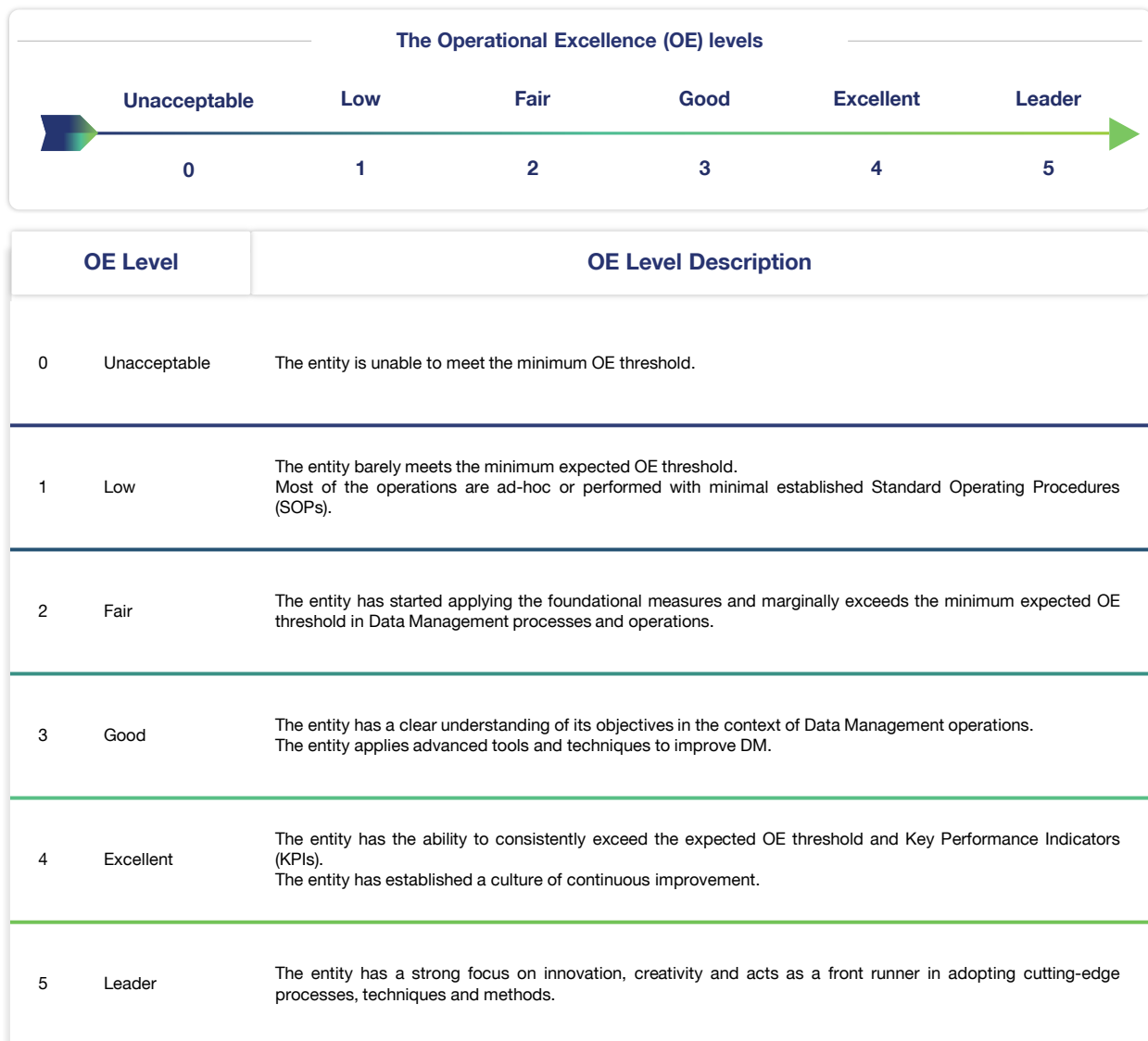
The compliance score is based on evaluating supporting evidence submitted by the entity on the NDI platform and its conformity with acceptance criteria. This evidence is assessed against 191 specifications outlined in the Data Management and Personal Data Protection (DM and PDP) Standards to reflect the entity's level of compliance. The NDI classifies the compliance score into two levels as follows:

Compliant	Non-Compliant
 An entity is considered compliant with the specification only when the supporting evidence fully meets the requirements.	 An entity is considered non-compliant with the specification if it has not met all the requirements. Partial implementation is considered in the compliance score if the entity has fulfilled part of the requirements.



6.3.3. The Score of the Operational Excellence (OE) Assessment

The OE component consists of several metrics that are divided across 6 of the DM domains listed under the scope (i.e., MCM, DQ, DO, DSI, RMD, OD, and more shall be added subsequently). The metric scores include different measurement units (e.g., Time, Percentage, etc.). In order to normalize the measurement units, each metric output is mapped to a predefined scale that ranges in value from **Level 0 “Unacceptable”** to **Level 5 “Leader”** which are described in the following figure:



▶ 7. Summary

In conclusion, SDAIA developed and launched the National Data Index (NDI), with its three component assessments which complement each other: Maturity, Compliance, and OE, in pursuit of improving the DM practices and processes in government entities and maximizing the value from data as a national asset. This contributes to leveraging data in informed decision-making, optimizing operational efficiency and achieving the national goal of becoming a leader in data-driven economies globally. Furthermore, OE increases the entity's progress in the DM processes and operations with the help of the National Data Platforms.

▶ 8. Appendix

This section consists of the detailed description of each NDI component which will have a separate score based on different measurements, thus contributing to the NDI outcomes:

▶ 8.1. Appendix I – DM Practices Maturity Assessment Questionnaire

This section provides a detailed questionnaire, which contains 42 questions aimed at evaluating entities' Data Management practices across 14 domains. Each domain has specific questions with maturity levels ranging from level 0 (Absence of capabilities) to 5 (Pioneer).

To demonstrate commitment to Data Management practices, the entities must provide SDAIA with acceptance evidences for each maturity level. This include a range of evidences, such as policies, reports, process documentation, implementation records, and other relevant artifacts. This will also help ensure compliance with Data Management and Personal Data Protection (DM and PDP) Standards.

8.1.1.Data Governance Domain

Maturity Questions – Data Governance Domain			
DG.MQ.1	Has the entity established & implemented a Data Management & Personal Data Protection (DM & PDP) Strategy and a DM & PDP Plan with Key Performance Indicators (KPIs) that can be continuously measured to ensure optimization?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No Data Management & Personal Data Protection (DM & PDP) strategy is in place.	- No required documents	
Level 1: Establishing	- The entity has existing DM practices that are not formalized (non-approved).	- Existing data-related practices.	
Level 2: Defined	- A cross-entity DM & PDP strategy is defined for all DM Domains. - DM Guiding principles have been developed.	- The approved DM & PDP Strategy.	- DG.1.1
		- The DM guiding principles.	- DG.1.2
		- Data Strategy Approval Decision.	- DG.1.4
Level 3: Activated	- The entity developed a DM & PDP implementation plan based on the defined DM & PDP strategy. - The entity is implementing this DM & PDP plan which covers all DM Domains.	All level 2 acceptance evidence requirements including: - The developed DM & PDP implementation plan.	- DG.1.3
		- Implementation status report.	
Level 4: Managed	- The entity is monitoring the DM & PDP strategy & plan implementation across all DM domains based on the pre-defined KPIs.	All level 3 acceptance evidence requirements including: - The monitoring report of the DM & PDP strategy & plan implementation based on the pre-defined KPIs in the strategy & implementation plan.	
Level 5: Pioneer	- The DM & PDP strategy is periodically updated, improved, and optimized across all DM domains based on the latest relevant practices in the field. - The DM & PDP implementation plan is periodically reviewed and updated based on the updates to the DM & PDP strategy and the changes in business requirements.	All level 4 acceptance evidence requirements including: - A report demonstrating that the entity monitors the latest DM practices, updates the implementation plan accordingly, and adjusts based on changes in business requirements.	- DG.6.1

Maturity Questions – Data Governance Domain			
DG.MQ.1	Has the entity established & implemented a Data Management & Personal Data Protection (DM & PDP) Strategy and a DM & PDP Plan with Key Performance Indicators (KPIs) that can be continuously measured to ensure optimization?		
Level Name	Level Description	Acceptance Evidence	Related Specification
		- A report demonstrating that the entity monitors the latest DM practices, updates the strategy accordingly, and adjusts based on changes in business requirements.	- DG.7.2

Maturity Questions – Data Governance Domain			
DG.MQ.2	Has the entity established and implemented Data Management (DM) Policies, Standards and Guidelines across all Data Management (DM) Domains?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No Data Management (DM) Policies, Standards, or Guidelines are in place.	- No required documents	
Level 1: Establishing	- The entity has existing DM-related policies and standards that are not formalized (non-approved). - The entity conducted a gap analysis to identify the required DM and PDP policies to be developed	- The Data Management & Personal Data Protection (DM & PDP) Policies, Controls, and Guidelines Gap Analysis document.	- DG.2.1
Level 2: Defined	- The entity has developed and approved policies, standards, and guidelines for all DM Domains.	All level 1 acceptance evidence requirements including: - The policies, standards, and guidelines developed by the entity for all DM domains.	- DG.2.2
Level 3: Activated	- The entity is implementing and adopting developed DM & PDP policies through defined procedures and standards to establish governance and standardize and manage compliance across the entity.	All level 2 acceptance evidence requirements including: - Implementation status report.	
		- A proof document of the entity's adoption of the developed policies, standards & guidelines.	
		- Approved Compliance Management Framework.	- DG.5.1
Level 4: Managed	- The DM and PDP policies, standards and processes are tracked and measured based on the pre-defined KPIs.	All level 3 acceptance evidence requirements including:	- DG.7.1 (3 & 6)

Maturity Questions – Data Governance Domain			
DG.MQ.2	Has the entity established and implemented Data Management (DM) Policies, Standards and Guidelines across all Data Management (DM) Domains?		
Level Name	Level Description	Acceptance Evidence	Related Specification
	- Periodic monitoring is conducted on the entity's compliance with the Regulations published by NDMO-SDAIA.	- Monitoring reports on the developed policies and standards based on the pre-defined KPIs related to these policies and standards, as outlined in the DM strategy and implementation plan.	
		- The Entity's Compliance Audit Results Report.	- DG.5.2
		- Compliance Monitoring Report.	- DG.5.3
Level 5: Pioneer	- The entity periodically reviews and updates its policies in accordance with relevant developments, in addition to adopting and implementing innovative mechanisms to enable efficient and effective compliance monitoring of the developed policies and standards.	All level 4 acceptance evidence requirements including: - A report demonstrating the entity's innovative mechanisms for enabling compliance monitoring of policies and standards related to DM & PDP.	

Maturity Questions – Data Governance Domain			
DG.MQ.3	Has the entity established and operationalized all roles required for the Data Management Organization as per the NDMO Controls & Specifications?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- The entity does not have an official/approved Data Management Organization structure in place.	- No required documents	
Level 1: Establishing	- The entity has established a Data Management Office and appointed a Chief Data Officer (CDO) and a Data Management/Data Governance officer.	- The entity's Data Management Office establishment decision letter.	- DG.4.1
		- The Hiring/Appointment decision letters of the following roles: A. Chief Data Officer (CDO).	- DG.4.3
		- The Hiring/Appointment decision letters of the following roles: B. Data Management Officer / Data Governance Officer.	- DG.4.4
Level 2: Defined	- The entity has formed a Data Management and Governance Committee, appointed a Compliance Officer, a Legal Advisor, and a designated Business Data Executive.	All Level 1 acceptance evidence requirements including: - Decision letters for forming a Data Management and Governance Committee	- DG.4.2
		- The Hiring/Appointment decision letters of the following roles: A. Compliance Officer.	- DG.4.6

Maturity Questions – Data Governance Domain

DG.MQ.3	Has the entity established and operationalized all roles required for the Data Management Organization as per the NDMO Controls & Specifications?		
Level Name	Level Description	Acceptance Evidence	Related Specification
		- The Hiring/Appointment decision letters of the following roles: B. Business Data Executive.	- DG.4.8
		- The Hiring/Appointment decision letters of the following roles: C. Legal Advisor.	- DG.4.11
Level 3: Activated	- All DM roles are established as per the DM and PDP Standards and fully adopted across the entity. - Data Stewardship / Ownership defined across the entity, in addition to providing business and technical support for critical Data systems & critical Data elements.	All Level 2 acceptance evidence requirements including: - The Hiring/Appointment decision letters of the following roles: A. Business Data Steward(s).	- DG.4.9
		- The Hiring / Appointment decision letters of the following roles: B. List of the IT Data Stewards.	- DG.4.10
		- The Hiring/Appointment decision letters of the following roles: C. Personal Data Protection (PDP) Officer.	- DG.4.7

Maturity Questions – Data Governance Domain

DG.MQ.3	Has the entity established and operationalized all roles required for the Data Management Organization as per the NDMO Controls & Specifications?		
Level Name	Level Description	Acceptance Evidence	Related Specification
		- The Hiring/Appointment decision letters of the following roles: D. Open Data and Information Access Officer.	- DG.4.5
		- The documented & approved Data Management Organization structure.	
		- The documented Data Stewardship / Ownership structure.	
Level 4: Managed	- The Data Management Organization & the structure are fully established and operationalized. - The roles are tracked through pre-defined KPIs, periodically updated and optimized.	All Level 3 acceptance evidence requirements including: - The monitoring reports for the Entity's Data Management Organization roles based on the pre-defined KPIs in the strategy & implementation plan	- DG.7.1 (KPI 1)
Level 5: Pioneer	- The entity periodically reviews and updates the roles and responsibilities of the DM Office staff, data owners, business data specialists, and IT data Stewards.	All level 4 acceptance evidence requirements including: - The continuous Improvement Report for the Roles and Responsibilities of Data Management Organization within the entity.	

Maturity Questions – Data Governance Domain			
DG.MQ.4	Has the entity established and implemented practices for Change Management including awareness, communication, change control, and capability development?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	No formal Change Management practices are in place.	No required documents	
Level 1: Establishing	- Awareness sessions, training courses and communication on DM-related practices are performed on a reactive and ad-hoc basis. - The entity has change control practices that are not formalized.	Evidences of communication on DM-related practices.	
		Evidences of training and awareness sessions conducted.	
Level 2: Defined	The entity has developed a change management plan at the organizational level for training, awareness, and communication regarding Data Management.	All level 1 acceptance evidence requirements including:	
		- The Change Management Plan covering all DM Domains including: A. The DM & PDP Training Plan for all DM Domains.	
		B. The DM Communication plan.	
		C. The Stakeholders engagement plan.	
Level 3: Activated	- The entity has announced the DM, DG, and PDP strategy to introduce and raise awareness about the strategy through various communication channels across the organization. - The entity is implementing the defined Change Management practices for all DM Domains - Formal communication channels are established and adopted for DM issues management, escalations, resolutions & approvals. - A Version control mechanism is defined and implemented for DM documents and artifacts that the entity published.	All level 2 acceptance evidence requirements including:	DG.3.1
		The Change Management Implementation Status Report showing the DM, DG & PDP Training and awareness-raising activities.	
		The Change Management Implementation Status Report showing the DM Communication activities.	- DG.6.2
		The Stakeholders Engagement and Socialization plan implementation status report.	- DG.1.4
		The Data Governance Approvals Register.	- DG.8.1

Maturity Questions – Data Governance Domain			
DG.MQ.4	Has the entity established and implemented practices for Change Management including awareness, communication, change control, and capability development?		
Level Name	Level Description	Acceptance Evidence	Related Specification
		- The Data Management Issue Tracking Register.	- DG.8.2
		- Evidences that the Entity has DM & DG document & artifact Version Control practices.	- DG.8.3
Level 4: Managed	- The entity is monitoring the progress and the effectiveness of the Change Management practices with pre-defined KPIs.	All level 3 acceptance evidence requirements including: - The monitoring report of the Change Management practices with pre-defined KPIs in the change management plan.	- DG.7.1 (KPIs 2, 4, 5, 7 & 8)
Level 5: Pioneer	- The entity periodically reviews, continuously updates, optimizes, and develops change management practices through adopting innovative mechanisms and methods for change management in areas related to data management.	All level 4 acceptance evidence requirements including: - The continuous Improvement Report of the Change Management, highlighting the innovative mechanisms contributing to change management in areas related to Data Management.	

8.1.2.Metadata and Data Catalog Domain

Maturity Questions – Metadata and Data Catalog Domain			
MCM.MQ.1	Has the entity developed and implemented a plan to integrate and manage Metadata across the entity?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No plan is in place to integrate and manage Metadata in the entity.	- No required documents	
Level 1: Establishing	- The entity manages its Metadata on a reactive and ad-hoc basis as needed.	- The Recorded or Documented Metadata Report.	
Level 2: Defined	- The entity developed a plan for the implementation of Metadata and Data Catalog. - The entity Defined a roadmap with a list of activities, required resources, and a budget to manage the Data Catalog and Metadata implementation.	- The Approved Metadata and Data Catalog Plan.	- MCM.1.1
		- The Approved Metadata Structure.	- MCM.4.3
Level 3: Activated	- The entity implements a recent, defined, and approved plan, along with a Metadata Structure defining the Metadata and Data Catalog. - This implementation includes the identification and prioritization of the critical systems and attributes.	All level 2 acceptance Evidence requirements, Including: - The Metadata and Data Catalog Plan Implementation Status Report.	
		- The approved Metadata Structure Implementation Report.	
Level 4: Managed	- The entity is monitoring the effectiveness of the Metadata and Data Catalog plan and activities with pre-defined Key Performance Indicators (KPIs).	All level 3 acceptance Evidence requirements, Including: - The Monitoring Report with Pre-defined Key Performance Indicators (KPIs) for the Metadata and Data Catalog Plan and Activities.	
Level 5: Pioneer	- The Metadata and Data Catalog plan and activities are regularly monitored for continuous improvement and optimization.	All level 4 acceptance Evidence requirements, Including:	

Maturity Questions – Metadata and Data Catalog Domain			
MCM.MQ.1	Has the entity developed and implemented a plan to integrate and manage Metadata across the entity?		
Level Name	Level Description	Acceptance Evidence	Related Specification
		- The Continuous Improvement Report on the Metadata and Data Catalog Plan.	

Maturity Questions – Metadata and Data Catalog Domain			
MCM.MQ.2	Has the entity implemented a Metadata Management and Data Catalog tool / solution?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No tools are in place to manage the entity's Metadata.	- No required documents	
Level 1: Establishing	- The entity manages its Metadata manually or in standalone applications without standardized tools.	- Evidences of current Existing Metadata.	
Level 2: Defined	- The entity documented its requirements for the Data Catalog tool / solution and selected an appropriate tool based on business and regulatory requirements. - The entity's data sources to be included in the Data Catalog tool have been identified and prioritized. - The entity developed a target Metadata architecture.	- The Selected Data Catalog Tool.	
		- The Approved and Prioritized Data Sources Report.	- MCM.1.2
		- The Developed and Approved Target Metadata Architecture.	- MCM.1.3
		- The Data Catalog Tool Implementation Requirements Report.	
		- The Approved and Developed Data Catalog Training Plan.	
Level 3: Activated	- The Data Catalog tool has been implemented and populated with the entity's Metadata. - The tool is integrated into the entity's Metadata repository with appropriate access permissions.	All level 2 acceptance Evidence requirements, Including: - Evidence of the Implemented Data Catalog Tool.	- MCM.5.1

Maturity Questions – Metadata and Data Catalog Domain			
MCM.MQ.2	Has the entity implemented a Metadata Management and Data Catalog tool / solution?		
Level Name	Level Description	Acceptance Evidence	Related Specification
	- The tool stores the activities and tracking logs for Audit Trails. - Power users are identified and trained on the Data Catalog tool usage. - A training and communication plan is rolled out to raise awareness and adoption of the Data Catalog tool. - The Data Catalog automated tool is regularly updated to the latest version.	- Data Access Approval Process Documentation (Authorization to Connect the Data Catalog with the Data Sources).	- MCM.2.1
		- Metadata Access Approval Process Documentation.	- MCM.2.2
		- Evidences of Data Catalog Adoption and Usage Including Metadata Populated on the Tool.	- MCM.3.2
		- The Regular Audits Report on the Data Catalog Usage.	- MCM.5.3
		- Evidence of Training Conducted for the Identified Data Catalog Users.	- MCM.3.1
		- Tool Versioning Report.	- MCM.5.4
Level 4: Managed	- The entity is monitoring changes to its Metadata through automated notifications. - The adoption and usage of the implemented Data Catalog tool is closely monitored based on a set of pre-defined Key Performance Indicators (KPIs).	All level 3 acceptance Evidence requirements, Including:	- MCM.6.1
		- The Monitoring Report with Pre-defined KPIs for the Adoption and Usage of the Metadata & Data Catalog Solution / Tool. - The Approved List of Pre-defined KPIs for the Quality of the Metadata which is Populated on the Data Catalog Tool.	
Level 5: Pioneer	- The entity has fully automated end-to-end Metadata (Business, Technical, and Operational) capture and exchange. - The entity continuously monitors and optimizes the Data Catalog. - The entity continuously updates the Data Catalog in the event of any changes specified by the National Data Bank (NDB).	All level 4 acceptance Evidence requirements, Including:	
		- The Continuous Improvement Report on the Metadata and Data Catalog Tool's quality. - The Metadata Management Automation Report.	

Maturity Questions – Metadata and Data Catalog Domain			
MCM.MQ.3	Has the entity defined and implemented formal processes for effective Metadata Management, such as: prioritization, population, access management, and quality issue management, etc., supported & fostered by collaboration across the entity?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No process is in place to manage Metadata.	- No required documents	
Level 1: Establishing	- The entity manages its Metadata on a reactive and ad-hoc basis as needed (e.g. Projects / initiatives) without formalized practices.	- Evidence of the Existing Processes Used to Manage Metadata.	
Level 2: Defined	- The entity defined processes to manage the Metadata across the business and technical applications. - The entity developed processes to prioritize, populate and manage the Metadata including access management, annotation, certification, and Metadata quality; by collaboration across the entity.	- Metadata Identification Process Report.	
		- Metadata Prioritization Process Report.	
		- Metadata Population Process Report.	- MCM.4.2
		- Metadata Update process Report.	- MCM.4.4
		- Metadata Quality process Report.	- MCM.4.5
		- Metadata Annotation process Report.	- MCM.4.6
Level 3: Activated	- The entity is implementing defined processes for end-to-end Metadata management. - The established processes for updating the Metadata are implemented and automated as workflows within the Data Catalog tool. - The Integrated Metamodel is deployed with role-based access. - The Metadata quality issues are identified and addressed. - Full end-to-end Metadata is collected and enriched. - All the Data Governance and Data Management teams along with business stakeholders are engaged collaboratively through the automated tool.	All level 2 acceptance Evidence requirements, Including: - Evidence of the Implementation and Adoption of the Approved Processes as Workflows in the Entity's Data Catalog.	
		- The Logs or the List of Notifications on the Metadata Changes.	- MCM.5.2
		- Evidences of Communications to the Data Catalog Users of any Metadata Update.	

Maturity Questions – Metadata and Data Catalog Domain			
MCM.MQ.3	Has the entity defined and implemented formal processes for effective Metadata Management, such as: prioritization, population, access management, and quality issue management, etc., supported & fostered by collaboration across the entity?		
Level Name	Level Description	Acceptance Evidence	Related Specification
		- The Metadata Stewardship Coverage Model.	- MCM.4.1
Level 4: Managed	- The entity is monitoring and tracking the Metadata processes and activities with pre-defined Key Performance Indicators (KPIs).	All level 3 acceptance Evidence requirements, Including:	
		- The Metadata Processes Monitoring Report with Pre-Defined KPIs.	
		- The Metadata Quality Monitoring Report with Pre-Defined KPIs.	- MCM.6.2
Level 5: Pioneer	- The entity's Metadata management processes and practices are regularly monitored for continuous improvement and optimization. - Optimization techniques are being utilized to improve the processes of developing taxonomies, ontologies, or semantic representations.	All level 4 acceptance Evidence requirements, Including: - The Continuous Improvement Report on the Metadata Management Practices.	

8.1.3.Data Quality Domain

Maturity Questions – Data Quality Domain			
DQ.MQ.1	Has the entity developed and implemented a Data Quality (DQ) plan focused on improving the quality of the entity's Data?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No formal Data Quality (DQ) plan is in place.	- No required documents	
Level 1: Establishing	- The entity implements Data Quality activities on a reactive or ad hoc basis.	- Evidence of the Existing Data Quality (DQ) Related Activities.	
Level 2: Defined	- The entity has a defined and approved DQ management plan. - A roadmap is defined with a list of activities, required resources, and a budget to manage the DQ implementation.	- The Defined and Approved DQ Implementation Plan.	- DQ.1.2
Level 3: Activated	- The entity is implementing the defined DQ plan and roadmap. - Clear roles and responsibilities are defined for the DQ activities in line with the Data Management Organization structure.	All level 2 acceptance Evidence requirements, Including: - A Report on the DQ Plan Implementation Status.	
		- A Report on the Defined DQ Roles & Responsibilities.	
		- A Report on the Assigned Resources for the DQ Plan.	
Level 4: Managed	- The entity is monitoring the implementation of the DQ plan and activities with the pre-defined Key Performance Indicators (KPIs).	All level 3 acceptance Evidence requirements, Including: - The Monitoring Report of the DQ Plan and Activities with Pre-defined Key Performance Indicators (KPIs).	
Level 5: Pioneer	- The DQ plan and activities are regularly monitored for optimization and continuous improvement. - DQ Management is embedded in the Data Lifecycle and Software Development Lifecycle (SDLC).	All level 4 acceptance Evidence requirements, Including: - The Continuous Improvement Report of the Data Quality Plan & Activities.	

Maturity Questions – Data Quality Domain			
DQ.MQ.2	Has the entity established / developed and implemented practices to manage and improve the quality of the entity's Data?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	No practices are in place for Data Quality (DQ).	No required documents	
Level 1: Establishing	- The entity has existing DQ-related practices that are not formalized. - The identification of data issues and the resolution activities are done on a reactive or ad hoc basis.	The Existing DQ Domain Initiatives.	
		The Existing Processes for Detecting DQ Issues.	
		The Existing Processes Used for Data Corrections or Data Validations.	
Level 2: Defined	- The entity prioritized Data elements based on the business requirements from the perspective of its importance for the DQ Management. - The entity defined DQ Dimensions for the prioritized datasets.	The Prioritized List of Data Elements.	- DQ.1.1
		The Defined DQ Dimensions for the Entity's Datasets.	- DQ.2.1
		The Data Quality Rules Report.	- DQ.2.1
	- The entity defined and documented DQ Rules including formats, mandatory fields, and validations for data-entry values. - The entity established DQ issue management processes to identify and resolve the DQ issues.	The Developed & Approved Processes for DQ Issue Management & Remediation.	- DQ.2.3
Level 3: Activated	- The entity is implementing DQ Management. - An initial DQ assessment was conducted to identify DQ issues. Periodic DQ assessments are established to ensure the improvement on the entity's DQ. - Data issues were identified, a root cause analysis was conducted and remediation activities were developed accordingly to correct the identified data issues. - Standardized DQ Tools are implemented with automated workflows and defined DQ Rules.	All level 2 acceptance Evidence requirements, Including: The Planned & Conducted Initial & Periodic Data Quality Assessment Report.	- DQ.1.3
		The Resolution Status Report of the Identified DQ Issues.	- DQ.2.3
		Evidences of DQ Tools Used for Automating DQ Issue Management Workflows.	- DQ.2.5
		The Defined & Implemented DQ Service Level Agreements (SLAs).	- DQ.2.4
		The List of DQ System Enforcements Adopted by the Entity.	

Maturity Questions – Data Quality Domain			
DQ.MQ.2	Has the entity established / developed and implemented practices to manage and improve the quality of the entity's Data?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 4: Managed	- The entity is monitoring the effectiveness of the DQ management practices with pre-defined KPIs. - The entity is monitoring the agreed upon DQ threshold values with pre-defined SLAs. - The entity is monitoring the effectiveness of the issue resolution process.	All level 3 acceptance Evidence requirements, Including: - The Monitoring Report of the DQ Management Practices with Pre-defined KPIs.	
		- The Monitoring Report of the DQ Threshold Values.	
		- The Monitoring Report of the DQ Issue Resolution Process.	- DQ.3.2
Level 5: Pioneer	- Proactive profiling and critical dataset identification are done using Advanced Artificial Intelligence / Machine Learning (AI/ML) based methods. - The DQ tools are continuously optimized to improve the DQ management processes. - Proactive remediation is done with proper monitoring of critical data systems, data entities (data objects) and data attributes. - The entity implemented DQ Management industry standards or developed entity-specific standards.	All level 4 acceptance Evidence requirements, Including: - The Continuous Improvement Report on the Tools Used for DQ.	
		- The Continuous Improvement Report on the DQ Management Practices.	
		- The Implemented / Adopted DQ Industry Standards.	

Maturity Questions – Data Quality Domain			
DQ.MQ.3	Has the entity established and implemented practices to monitor and report the entity's Data Quality (DQ) status?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No practices are in place to monitor nor report on the quality of data.	- No required documents	
Level 1: Establishing	- The entity monitors its DQ on a reactive or ad hoc basis.	- The Existing DQ Monitoring Practices.	

Maturity Questions – Data Quality Domain			
DQ.MQ.3	Has the entity established and implemented practices to monitor and report the entity's Data Quality (DQ) status?		
Level Name	Level Description	Acceptance Evidence	Related Specification
		- Evidence of the Entity's Current DQ Status.	
Level 2: Defined	- The entity defined and formalized DQ monitoring and reporting practices to maintain and document the DQ activities on a regular basis. - The entity developed DQ processes and a plan for conducting DQ Audits at defined checkpoints.	- The Defined and Formalized DQ Monitoring Plan.	- DQ.2.2
		- The Defined DQ Checkpoints Report.	
Level 3: Activated	- The entity is monitoring the quality of its data and documenting the quality status on a regular basis. - DQ reviews are conducted at the defined DQ Checkpoints. - A workflow for reporting DQ issues has been implemented on the Data Catalog automated tool. - The DQ Rules and the DQ Monitoring results are documented as the Metadata within the Data Catalog automated tool.	All level 2 acceptance Evidence requirements, Including:	- DQ.2.2
		- DQ Scorecards or Dashboards.	
		- A Report on the Data Quality Metadata Logged on the Data Catalog Tool.	- DQ.4.3
		- Evidence of a Data Quality Support Process Implemented as a Workflow.	- DQ.4.2
Level 4: Managed	- The entity monitors the DQ trends and reporting activities based on pre-defined KPIs and established targets.	All level 3 acceptance Evidence requirements, Including:	- DQ.3.1
		- Trends from the DQ Monitoring Activities with Pre-defined KPIs.	
Level 5: Pioneer	- The entity conducts periodic reviews of the monitoring and reporting practices for continuous improvement in line with the changes in business and technical requirements.	All level 4 acceptance Evidence requirements, Including: - The continuous Improvement Report on the DQ Monitoring and Reporting Practices.	

Maturity Questions – Data Quality Domain			
DQ.MQ.4	Has the entity developed Data Quality (DQ) standards, provided definitions for its datasets, and published / uploaded the definitions on the National Data Catalog (NDC)?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	No standards nor definitions are in place for the entity's datasets.	No required documents	
Level 1: Establishing	The entity defines its datasets and DQ standards on an ad hoc / project basis.	The Existing List of Data Standards and Data Definitions.	
Level 2: Defined	- The entity has data definitions and standards for a set of domains / attributes in line with the DQ Dimensions. - The entity identified and provided Metadata definitions for all data attributes in line with the DQ definitions. - The entity identified the datasets for which Metadata should be published on the National Data Catalog (NDC).	- The Developed Data Standards for Data Elements. - The Identified Metadata with their Definitions. - The Identified datasets to be Published on the National Data Catalog (NDC).	
Level 3: Activated	- The entity has been on boarded on the NDC. The entity populated the Metadata definitions on the NDC. - The entity is developing and implementing standards independently for the entity-specific domains / attributes. - The entity uploads the Metadata on the NDC as required.	All level 2 acceptance Evidence requirements, Including: - A Report about the Data Standards & the Data Definitions which the Entity Uploaded on the NDC. - The Entity-Specific List of Applied Data Definitions and Applied Data Standards.	
Level 4: Managed	The entity's data definitions and data standardization processes are reviewed and tracked through pre-defined KPIs.	All level 3 acceptance Evidence requirements, Including: A Monitoring Report for the Data Definitions and Data	

Maturity Questions – Data Quality Domain			
DQ.MQ.4	Has the entity developed Data Quality (DQ) standards, provided definitions for its datasets, and published / uploaded the definitions on the National Data Catalog (NDC)?		
Level Name	Level Description	Acceptance Evidence	Related Specification
		Standardization with Pre-defined KPIs.	
Level 5: Pioneer	- The standards are developed proactively for all the new and future systems. The standards are continuously improved across the entity's data systems. - Regular assessments are conducted to ensure that the standards and definitions are provided and implemented for the entity's datasets.	All level 4 acceptance evidence requirements, including: - The Continuous Improvement Report for optimizing the data standards and definitions within the entity and on the NDC.	

8.1.4.Data Operations Domain

Maturity Questions – Data Operations Domain			
DO.MQ.1	Has the entity developed and implemented a plan to manage and satisfy the needs of Data Operations, Data storage and Data retention?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	No plan is in place for Data Operations (DO), Data storage, Data retention and disaster recovery (DR).	No required documents	
Level 1: Establishing	The entity has existing practices for Data Operations, storage and retention. However, this plan is setup in a reactive form on an ad hoc basis.	The Approved initial data operations and storage plan.	
Level 2: Defined	- The entity has a defined and approved Data Operations (DO) and storage plan and roadmap including: - Data storage forecasting. - Budget and resource allocation. - Information systems prioritization. - The DO plan should be in line with: - The policy development. - Tool selection. - Business continuity. - Plans for backup and disaster recovery.	The Developed and Approved Data Operations and Storage Plan.	- DO.1.1
		The Information Systems Priority List.	- DO.1.3
		The Developed and Approved Policies for Data Operations, Storage, Retention and Business Continuity.	- DO.2.1
		The Periodic Forecasting Plan for Storage Capacity.	- DO.1.2
		The Database Technology Evaluation Process and Selection Criteria.	- DO.1.4
Level 3: Activated	- The entity is implementing its defined Data Operations (DO) plan. - The entity assigned & activated the roles and responsibilities to manage the DO, storage and retention in line with the business requirements and the overall "Data Management Organization" structure. - The entity is reporting on the database performance.	All level 2 acceptance Evidence requirements, Including: The Data Operations and Storage plan with implementation status report.	
		The Storage Trend Forecast Document.	- DO.1.2

Maturity Questions – Data Operations Domain

DO.MQ.1	Has the entity developed and implemented a plan to manage and satisfy the needs of Data Operations, Data storage and Data retention?		
Level Name	Level Description	Acceptance Evidence	Related Specification
	- The entity is conducting periodic forecasts of its storage capacity.	- The Database Technology Evaluation Report.	- DO.1.4
		- The Document on the Entity's Application Performance Assessment.	
		- The Entity's Applications Development Roadmap with the Status Report on the Implementations.	
		- The Budget Estimations of the Procurement Transactions of the Future Storage Needs.	
		- The Data Operations Orchestration Document.	
Level 4: Managed	- The entity is monitoring the progress and effectiveness of the Data Operations (DO) plan implementation with pre-defined Key Performance Indicators (KPIs).	All level 3 acceptance Evidence requirements, Including: - The Monitoring Report with Pre-defined Key Performance Indicators (KPIs) for the Implementation Progress and Effectiveness of the Data Operations Plan.	- DO.5.1
Level 5: Pioneer	- The entity's Data Operations (DO), storage, retention and recovery practices are continuously reviewed and optimized.	All level 4 acceptance Evidence requirements, Including: - The Continuous Improvement Report on the Practices of Data Operations, Storage, and Retention.	

Maturity Questions – Data Operations Domain			
DO.MQ.2	Does the entity have in place a defined methodology, processes and Standard Operating Procedures (SOPs) for database operations?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	No practices nor processes are in place for database management and operations.	No required documents	
Level 1: Establishing	- The entity conducts Data Operations but not in a standardized approach. - Operations are being managed without clear procedures or with minimal documented procedures.	Evidences of Data Operations Done within the Entity.	
Level 2: Defined	- The entity has defined and developed practices and processes for database operations management, monitoring and storage configurations including access control processes for the databases. - All roles and support levels are identified to manage the database operations. - Processes and Standard Operating Procedures (SOPs) are documented with clearly defined roles and responsibilities across the operations and the IT teams. - The Database Management System (DBMS) / tool is regularly updated to the latest version. - Service Level Agreements (SLAs) are developed to guide the database operations.	- The Process Documentation of the Detailed Practices of Data Operations, Including: A. Database Monitoring.	DO.3.1
		B. Database Access Control.	DO.3.2
		C. Storage Configuration Management.	DO.3.3
		D. DBMS Versioning Mechanism.	DO.3.4
		E. The Database Performance Service Level Agreements and Operational Level Agreements (SLAs & OLAs).	
Level 3: Activated	- The entity is implementing the defined Practices and Processes of Database operations management and Storage Configurations. - Under these Processes within the entity, there are Standard Operating Procedures (SOPs) include: - The database performance monitoring and reporting. - Role-based access control. - Storage Configuration Management and DBMS versioning (Implementation of database changes on the Production Environments). - The Standard Operating Procedures (SOPs) are activated:	- All level 2 acceptance Evidence requirements, Including: - The Database Monitoring Status Report.	DO.3.1
		The Data Operations operating model.	
		Evidences of Agreements (SLAs and OLAs).	DO.3.5

Maturity Questions – Data Operations Domain			
DO.MQ.2	Does the entity have in place a defined methodology, processes and Standard Operating Procedures (SOPs) for database operations?		
Level Name	Level Description	Acceptance Evidence	Related Specification
	- For all support levels, communication, escalation and resolution. - With all the involved stakeholders. - All required Data Operations (DO) roles are activated and onboarded. - The Service Level Agreements (SLAs) and the Operational Level Agreements (OLAs) are enforced as agreed upon with business stakeholders.		
Level 4: Managed	The entity is monitoring the DO processes and SOP with pre-defined Key Performance Indicators (KPIs) and thresholds.	All level 3 acceptance Evidence requirements, Including: The Monitoring Report with Pre-defined KPIs for Database Operations Management.	
Level 5: Pioneer	- DO and Storage practices and processes are continuously reviewed and optimized. - Leading DO practices are evaluated on a regular basis and adopted (e.g., DataOps). - All operational metrics covering SLAs / OLAs, and Key Performance Indicators (KPIs) / Key Quality Indicators (KQIs) are reviewed proactively to improve and optimize the operations. - Proactive / preventive measures are planned and executed to ensure uninterrupted operations. - All learning scenarios and experiences cases are documented and updated regularly to create a knowledgebase for reusability and future planning.	All level 4 acceptance Evidence requirements, Including: - The Continuous Improvement Report on the Implemented Practices and Processes of Data Operations and Storage. - The Knowledgebase document.	

Maturity Questions – Data Operations Domain			
DO.MQ.3	Does the entity have in place, practices and processes for Business Continuity such as backup and disaster recovery (DR) and a defined Business Continuity Plan (BCP) for the data?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	No plans, practices or processes are in place for business continuity such as backups and disaster recovery.	No required documents	
Level 1: Establishing	The entity's data backup and disaster recovery practices are reactive and on an ad hoc basis.	Evidences of Data Storage Backup Instruction Documents.	

Maturity Questions – Data Operations Domain			
DO.MQ.3	Does the entity have in place, practices and processes for Business Continuity such as backup and disaster recovery (DR) and a defined Business Continuity Plan (BCP) for the data?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 2: Defined	- The entity has defined and developed plans, practices and processes for business continuity, data backup, and disaster recovery in line with the DM and PDP standards. - The Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) for the critical systems are defined (e.g., backup frequency, location of backup files, storage medium and scope).	- The Developed Processes and Practices for Data Storage Backups and Recovery.	- DO.4.1
		- The Business Continuity Plan (BCP) and Processes.	
		- The Disaster Recovery (DR) Processes and Plan.	- DO.4.2
		- A Document of Actions Required to Implement Database Changes and Rollbacks.	
Level 3: Activated	- The entity is implementing its defined Business Continuity Plan (BCP), practices and processes for business continuity, data backup and recovery. - The BCP is implemented for the critical systems. - Role-based access control for production data, all RTO / RPO details (High availability, load balancing, etc.) are agreed upon with Business and IT stakeholders and implemented. - The Incident response teams are activated.	All level 2 acceptance Evidence requirements, Including:	
		- The Technical Design Document.	
		- The BCP Run Report.	
		- Disaster Recovery Plan Run Report (DR Run Report).	
		- The Change Request for Production Data.	
		- The Production Data Access Control Document.	- DO.4.3
Level 4: Managed	- The entity is monitoring the practices pertaining to the BCP and DR with pre-defined Key Performance Indicators (KPIs).	All level 3 acceptance Evidence requirements, Including: - The Monitoring Report with Pre-defined KPIs for the Business Continuity (BCP) and Disaster Recovery (DR).	

Maturity Questions – Data Operations Domain			
DO.MQ.3	Does the entity have in place, practices and processes for Business Continuity such as backup and disaster recovery (DR) and a defined Business Continuity Plan (BCP) for the data?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 5: Pioneer	- The entity continuously reviews data storage backup & recovery and disaster recovery processes for improvement and optimization. - The entity performs periodic executions and validations of the RTO and RPO to ensure that the systems are well prepared for any unexpected interruption or calamity. - The BCP details are regularly reviewed to incorporate the learnings, modern trends and business needs / demands.	All level 4 acceptance Evidence requirements, Including: - The Continuous Improvement Report on the Business Continuity Plan (BCP).	

8.1.5.Document and Content Management Domain

Maturity Questions – Document and Content Management Domain			
DCM.MQ.1	Has the entity developed a Document and Content Management (DCM) plan and a Digitization plan to manage the implementation of paperless management activities?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- The entity doesn't have any plan in place currently for Document and Content Management (DCM).	- No required documents	
Level 1: Establishing	- The entity manages documents and content on a reactive or ad hoc basis without formalized DCM practices.	- Evidences of Existing DCM Activities.	
Level 2: Defined	- The entity has defined plans to manage the entity's documents and content lifecycle and digitization activities. A roadmap has been defined with a list of activities, required resources, trainings, awareness and a budget to manage both DCM and Digitization. - The entity has defined processes for prioritizing and digitizing documents to be stored in the entity's Document Management System (DMS). - The entity has identified and prioritized the key processes to be implemented as workflows in DMS to enable automated and paperless management of documents.	- The DCM Plan.	- DCM.1.1
		- The DCM Digitization Plan.	- DCM.1.2
		- The Developed DCM Training Plan.	
		- The Developed Prioritization Process for Documents and Content.	
		- The Identified DCM Processes / Procedures.	- DCM.1.4
		- The Ranked List of Prioritized Document Workflows to be Implemented.	- DCM.1.4
Level 3: Activated	- The entity is implementing its DCM plan and Digitization plan including training and awareness activities. - The entity is prioritizing its documents to be stored in the entity's Document Management System (DMS). - Roles and responsibilities are defined and initiated to manage the DCM activities and the Digitization activities in line with the overall "Data Management Organization" structure.	All level 2 Acceptance Evidences required including:	
		- The DCM Plan Implementation Status Report.	
		- The Digitization Plan Implementation Status Report.	
		- The List of Prioritized Documents for Digitization.	- DCM.1.3
		- The DCM Roles and Responsibilities.	
		- The DCM Training Plan Implementation Status Report.	- DCM.3.1

Maturity Questions – Document and Content Management Domain			
DCM.MQ.1	Has the entity developed a Document and Content Management (DCM) plan and a Digitization plan to manage the implementation of paperless management activities?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 4: Managed	The entity is monitoring the effectiveness of the DCM plan and the DCM Digitization plan with pre-defined Key Performance Indicators (KPIs).	All level 3 Acceptance Evidences required including: The Monitoring Reports with Pre-defined KPIs for the Implementation of the DCM Plan & the DCM Digitization Plan.	
Level 5: Pioneer	The entity continuously reviews and updates both its DCM plan and Digitization plan for improvement and optimization in line with the changing business needs.	All level 4 Acceptance Evidences required including: The Continuous Improvement Report of the DCM and Digitization plans.	

Maturity Questions – Document and Content Management Domain			
DCM.MQ.2	Has the entity implemented policies and processes for Document and Content Management (DCM) including: Backup & Recovery, Retention & Disposal, Document & Content Access Approval, and Metadata Publishing?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	No policies and processes are in place currently for Document and Content Management (DCM).	No required documents	
Level 1: Establishing	The entity manages its documents and content on a reactive and ad hoc basis without formalized DCM policies and processes.	Evidences of Processes for Retaining & Disposing of Documents.	
Level 2: Defined	- The entity defined a clear set of policies and processes to manage its documents and content. - The Processes are defined for: - Backup & Recovery. - Retention & Disposal. - Document and Content Access Approvals. - Metadata Publishing.	The Developed Policy Document for the DCM Lifecycle.	- DCM.2.1
		The Developed DCM Backup & Recovery Procedures.	- DCM.4.1
		The Developed DCM Retention & Disposal Procedures.	- DCM.4.2
		The Developed DCM Role-Based Access Approval Procedures	- DCM.4.3
		The Developed DCM Metadata Publishing Procedures.	
Level 3: Activated	The entity is implementing its DCM processes aligned with the policies.	All level 2 Acceptance Evidences required including:	- DCM.4.2

Maturity Questions – Document and Content Management Domain			
DCM.MQ.2	Has the entity implemented policies and processes for Document and Content Management (DCM) including: Backup & Recovery, Retention & Disposal, Document & Content Access Approval, and Metadata Publishing?		
Level Name	Level Description	Acceptance Evidence	Related Specification
	- The Document Management System (DMS) is included in the entity's Backup & Recovery plan. - Documents are transferred to the entity's archival facility (Archival Register). - The physical destruction and deletion of the documents is done securely. - The entity established role-based access authorizations to the Content Management System (CMS) and the Document Management System (DMS). - Document and content Metadata is published via an automated tool. - Periodic DCM audits are conducted to ensure that the right information is getting to the right people at the right time.	- The Implemented Workflow for the DCM Retention & Disposal Process.	
		- The Implemented Workflow for the DCM Access Approval Process.	- DCM.4.3
		- Evidences of Document Transfers to the Archival Facility (Archival Register).	
		- The Documents Disposal Register.	
		- The Access Rights Documentation.	
		- The Report on Document & Content Metadata Publishing.	- DCM.4.4
Level 4: Managed	- The entity is monitoring the DCM processes aligned with the policies with pre-defined Key Performance Indicators (KPIs). - The Audit Trail / Audit Framework is tracked based on pre-defined Key Performance Indicators (KPIs).	All level 3 Acceptance Evidences required including: - The Monitoring Report with Pre-defined Key Performance Indicators (KPIs) of the DCM Processes Aligned with the Policies.	- DCM.5.1
Level 5: Pioneer	- The entity regularly reviews and updates its DCM processes for continuous improvement and optimization.	All level 4 Acceptance Evidences required including: - The Continuous Improvement Report on the DCM Processes and Practices.	

Maturity Questions – Document and Content Management Domain			
DCM.MQ.3	Has the entity implemented a tool to support Document and Content Management (DCM) processes including Digitization Management implementation?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No tools are in place currently for managing documents nor content.	- No required documents	

Maturity Questions – Document and Content Management Domain			
DCM.MQ.3	Has the entity implemented a tool to support Document and Content Management (DCM) processes including Digitization Management implementation?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 1: Establishing	- The entity manages documents and content in disparate applications.	- Evidences of Document Storage / Retention & Disposal Activities.	
Level 2: Defined	- The entity identified and developed or acquired the required tool to support DCM.	- The documented DCM tool requirements.	
Level 3: Activated	- The entity implemented the selected tool for Document and Content Management (DCM) which includes: • A Document Management System (DMS). • A Web Content Management System (CMS). • A collaboration tool.	All level 2 Acceptance Evidences required including:	- DCM.4.5
		- The Implemented Tool for DCM.	
		- The Record of Digitized Documents.	
Level 4: Managed	- The entity is monitoring the implementation of the tool based on pre-defined Key Performance Indicators (KPIs).	- The List of Approved Users.	
		All level 3 Acceptance Evidences required including:	
Level 5: Pioneer	- For Continuous Improvement, the entity regularly reviews: • The performance of the implemented Digitization Management tool to ensure automation. • The DCM activities to ensure optimization.	- The Monitoring Report on the Implemented Tool with Pre-defined Key Performance Indicators (KPIs).	
		All level 4 Acceptance Evidences required including:	
		- The Continuous Improvement Report on the DCM Solution / Tool Design and DCM Practices.	

8.1.6.Data Architecture and Modelling Domain

Maturity Questions – Data Architecture and Modelling Domain			
DAM.MQ.1	Has the entity developed and implemented a plan to improve its Data Architecture Capabilities?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No plan is in place for Data Architecture & Modelling (DAM).	- No required documents	
Level 1: Establishing	- The entity manages its Data Architecture & Modelling (DAM) related activities on a reactive and ad-hoc basis without formalized practices.	- The existing DAM Domain related practices.	
Level 2: Defined	- The entity has a defined & approved DAM Management plan. - The entity developed an entity-wide baseline current state and target future state Data Architecture in accordance with the Enterprise Architecture (EA). - The entity performed a gap analysis resulting in an implementation roadmap with defined priorities. - The entity adopted a Standard enterprise architecture framework. - The entity published its DAM Policies & Guidelines.	- The Approved Current State Data Architecture & the Existing Technical Architecture.	- DAM.3.1
		- The Approved Target State Data Architecture.	- DAM.3.2
		- The Future State Gap Assessment.	- DAM.3.3
		- The Approved DAM Plan.	- DAM.1.1
		- The Approved Enterprise Architecture Framework.	
		- The DAM Policy.	- DAM.2.1
Level 3: Activated	- The entity is implementing the defined implementation roadmap for its Target State Data Architecture. - The IT architecture is ensuring all business architecture outcomes are addressed by selecting and implementing the right technical capabilities. - The Business Architecture team works closely with the entity's Enterprise Architecture team to align the applicable Standards (e.g., DMBOK, TOGAF, etc.).	All level 2 acceptance evidence requirements including: - The DAM Plan Implementation Progress Report.	
		- The EA Framework Implementation Report.	

Maturity Questions – Data Architecture and Modelling Domain			
DAM.MQ.1	Has the entity developed and implemented a plan to improve its Data Architecture Capabilities?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 4: Managed	The entity is monitoring the effectiveness of the DAM Plan & activities with pre-defined Key Performance Indicators (KPIs).	All level 3 acceptance evidence requirements including: The Monitoring Report of the DAM Plan & Activities Implementation with Pre-defined KPIs.	DAM.6.1
Level 5: Pioneer	- The entity follows an identified architecture Change Management process to review, approve and implement the changes to the Current and / or Target State Data Architectures. - The entity continuously reviews the Target State Data Architecture via checkpoints incorporated into the Software Development Lifecycle (SDLC) process. - The entity regularly reviews and refines the Target State roadmap, priorities, and architecture artifacts, reflecting the current Enterprise Architecture strategy and key initiatives.	All level 4 acceptance evidence requirements including: The Data Architecture Plan's Continuous Improvement Report.	
		The Architecture Change Management Process.	DAM.5.1
		The Change Control Document.	
		The Data Architecture Checkpoints Report.	DAM.5.2

Maturity Questions – Data Architecture and Modelling Domain			
DAM.MQ.2	Has the entity developed and implemented practices for Data Architecture & Modelling (DAM) activities (including Data Flows, Data Models and Governance considerations)?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	No practices are in place within the entity for Data Architecture & Modelling (DAM).	No required documents	
Level 1: Establishing	- The entity maps Data Flows to the business processes, as needed, only on a reactive basis for specific projects / initiatives. - The entity documents Data Models, as needed, only on a reactive basis for specific projects/initiatives.	The Current Data Flows and Models Activities.	
Level 2: Defined	- The entity has identified & defined the requirements for developing a Data Lake environment. - The entity has defined a Partitioning Strategy for the target state data architecture. - The entity identified and mapped its Data Flows to the business processes.	A document containing the Approved Business Processes on the Data Architecture and any Related Data Flow.	
		A document containing the Big Data Considerations Including the Data Lake Requirements.	DAM.3.4

Maturity Questions – Data Architecture and Modelling Domain			
DAM.MQ.2	Has the entity developed and implemented practices for Data Architecture & Modelling (DAM) activities (including Data Flows, Data Models and Governance considerations)?		
Level Name	Level Description	Acceptance Evidence	Related Specification
	- The entity's Enterprise Data Model adopts a Standard diagramming approach (e.g. UML) for documenting the structure, relationships, and notations of business entities at the conceptual, logical and physical levels. - The entity stores in a register, its Data & Technical Architecture projects, Reference documentation materials, and Data Model designs. - The end-to-end Data Modelling lifecycle is defined with required processes and best practices / guidelines such as naming conventions, Data types, physical model deployment considerations and optimizations, etc.	- A document containing the Data Processing Considerations Including the Partitioning Strategy.	- DAM.3.5
		- Model representation.	- DAM.4.1
		- The DAM Register.	- DAM.7.1
		- A document containing the Data Model Representation's Technical Standards & Best Practices.	
Level 3: Activated	- The entity is implementing the defined practices for its DAM activities. - Multiple data integration and flow patterns are designed, published and operated according to defined Data Architecture principles such as "Capture Once Use Many" etc. - Structured and streamlined information flows across the entity are done using the defined and published data integration patterns. - The entity is implementing tools and technologies for DAM initiatives. - Data Models are uploaded in the Data Catalog. - The Logical Model is linked with business glossaries and technical attributes to provide end-to-end lineage and activate the impact analysis.	All level 2 acceptance evidence requirements including:	
		- The Data Integration Pattern Implementation Document.	
		- Evidences of DAM Tools & Technologies in Use.	- DAM.4.2
		- Evidences of the Enterprise Data Model Uploaded in the Data Catalog.	
	- The entity's Enterprise Data Model is used throughout the Software Development Lifecycle (SDLC). - The development is done via a Data Model tool.	- Evidences of Applying the Technical Data Standards.	

Maturity Questions – Data Architecture and Modelling Domain			
DAM.MQ.2	Has the entity developed and implemented practices for Data Architecture & Modelling (DAM) activities (including Data Flows, Data Models and Governance considerations)?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 4: Managed	- The entity is monitoring the implementation of the DAM practices with pre-defined Key Performance Indicators (KPIs).	All level 3 acceptance evidence requirements including: - The Monitoring Report of the Implementation of the DAM Practices with Pre-defined KPIs.	
Level 5: Pioneer	- The mapping of the entity's Data Flow to the Business processes is continuously monitored, measured, and improved including: • Multi-latency, multi-format Data Flows & Architecture Patterns defined, adopted, and mapped to the business processes. • Entity-wide data structures and data services mapped to the business processes. • Entity-wide data structures and data services shared instantly in real-time.	All level 4 acceptance evidence requirements including: - The Continuous Improvement Report Including the DAM Business Process Documentation.	

8.1.7. Data Sharing & Interoperability Domain

Maturity Questions – Data Sharing & Interoperability Domain			
DSI.MQ.1	Has the entity developed and implemented a Data Sharing and Integration (DSI) Plan in line with the Data Sharing Policies?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No plan is in place for Data Sharing nor Integration.	- No required documents	
Level 1: Establishing	- The entity shares data as needed on a reactive or ad-hoc basis.	- The list of Current Practices of Data Sharing and Integration (DSI).	

Maturity Questions – Data Sharing & Interoperability Domain			
DSI.MQ.1	Has the entity developed and implemented a Data Sharing and Integration (DSI) Plan in line with the Data Sharing Policies?		
Level Name	Level Description	Acceptance Evidence	Related Specification
	- Manual data exchange practices exist within the entity and with other Entities. - The entity conducted an initial assessment of data integration to identify pain points and inefficiencies in data movement flow and integration across the organization.	- The Updated and Approved Results of the Initial Data Integration Assessment.	- DSI.1.1
Level 2: Defined	- A Target Data Integration Architecture was developed based on the identified pain points. - The entity has developed an integration strategy and implementation plan for data sharing and integration to remediate the identified pain points and manage the required integration initiatives. - The Data Sharing policies and guidelines are defined for DSI within and outside the entity in line with the Data Sharing Regulations published by NDMO-SDAIA. - The entity has developed a plan for training every employee involved in the Data Sharing initiatives.	All level 1 acceptance evidence requirements including:	
		- The Developed Data Integration Strategy Document.	
		- The Developed Target Data Integration Architecture.	- DSI.1.2
		- The Developed Data Integration Plan (Including Data Sharing Activities).	- DSI.1.3
		- The Developed Data Sharing Policies.	
Level 3: Activated	- The entity is implementing the defined plan and roadmap for data sharing and integration. - Roles and responsibilities are assigned within the entity to manage Data Sharing requests and data integration activities in line with both the Data Management Organization structure and the Data Sharing regulations published by NDMO-SDAIA. - The entity is conducting Data Sharing training in line with the Data Sharing training plan.	All level 2 acceptance evidence requirements including:	
		- A Data Integration Plan Implementation Status Report.	
		- A Report on the Defined Roles and Responsibilities for DSI.	
		- A Progress Report on Data Sharing Training Programs.	DSI.2.1

Maturity Questions – Data Sharing & Interoperability Domain			
DSI.MQ.1	Has the entity developed and implemented a Data Sharing and Integration (DSI) Plan in line with the Data Sharing Policies?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 4: Managed	- The entity is monitoring the implementation of the DSI activities to ensure completion according to the plan with pre-defined Key Performance Indicators (KPIs).	All level 3 acceptance evidence requirements including: - The Monitoring Report with Pre-defined Key Performance Indicators (KPIs) for the Data Integration Plan and Data Sharing Activities.	
Level 5: Pioneer	- The DSI plan and the activities are continuously optimized to facilitate innovation and to maintain compliance with the Data Sharing Policies.	All level 4 acceptance evidence requirements including: - The Continuous Improvement Report on the Data Integration Plan and Data Sharing Activities.	

Maturity Questions – Data Sharing & Interoperability Domain			
DSI.MQ.2	Has the entity defined and implemented Processes for Sharing Data within the entity and with other Entities?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No processes are in place for sharing the entity's data internally or externally.	- No required documents	
Level 1: Establishing	- The entity shares data internally & externally as needed, on a reactive or ad-hoc basis with no formalized practices.	- Evidences of the Current DSI Practices / Processes by the Entity (Internally & Externally).	
Level 2: Defined	- The entity defined and approved a standardized Data Sharing mechanism for sharing data internally and externally according to the defined classification levels. The mechanism includes forms, processes and agreements to be used to manage the Data Sharing requests in line with the Data Sharing principles and regulation. - Data Sharing request forms have been developed and are shared with Data requestors as needed. - The Data Sharing agreements have been developed for Internal and External Data Sharing.	- The Process Documentation for Data Sharing (Including Data Classification Levels and Timelines).	- DSI.5.1
		- The Developed and Approved Data Sharing Request Forms (Internal and External).	
		- The Developed and Approved Internal Data Sharing Agreement Template.	- DSI.7.1
		- The Developed and Approved External Data Sharing Agreement Template.	- DSI.7.2
Level 3: Activated	- The entity is implementing and operationalizing the defined and approved Data Sharing mechanism to facilitate Data Sharing within and outside the entity. - Data is shared with entities only through SDAIA's certified and approved channels (e.g., The Government Service Bus (GSB), National Information Center Network, etc.). In alignment with the Data Sharing Policy issued by the National Data Management Office at SDAIA.	All level 2 acceptance evidence requirements including: - Evidences of Operationalization of The Data Sharing Process, e.g.: Communication of The Defined Data Sharing Mechanism.	- DSI.5.1
		- Evidences of Data Sharing Through SDAIA's Certified and Approved Channels.	

Maturity Questions – Data Sharing & Interoperability Domain			
DSI.MQ.2	Has the entity defined and implemented Processes for Sharing Data within the entity and with other Entities?		
Level Name	Level Description	Acceptance Evidence	Related Specification
	- The entity put in place controls to ensure that only the appropriate authority is allowed to access, obtain and use the shared data based on the nature and sensitivity of the data. - All ongoing Data Sharing agreements are reviewed on a regular basis to accommodate for any changes. - The entity's official Government website has an established channel to manage Data Sharing requests.	- The Access Authorization Controls Document.	
		- Evidences of Data Sharing Requests Submitted to The Entity and The Requests Submitted by The Entity Through the Established Channel.	- DSI.6.1
		- Evidences of the Entity's Responses to the Data Sharing Requests.	
		- An Adoption Evidence of The Developed Data Sharing Agreement Template for An Internal Data Sharing Request.	- DSI.7.1
		- An Adoption Evidence of The Developed Data Sharing Agreement Template for An External Data Sharing Request.	- DSI.7.2
		- The Documented Review Outcomes of The Data Sharing Agreements.	- DSI.7.3
Level 4: Managed	- The entity is measuring the efficiency of Data Sharing activities, tracking progress, and ensuring compliance with pre-defined KPIs.	All level 3 acceptance evidence requirements including: - The Monitoring Report with Pre-defined KPIs for the Data Sharing Processes.	- DSI.8.1 (3,4,5,6,7)
		- The compliance audit methodology.	
Level 5: Pioneer	- The entity's Data Sharing process is automated and updated frequently. - Data Sharing practices are regularly reviewed and adjusted to address the changing business objectives while implementing continuous improvements.	All level 4 acceptance evidence requirements including: - The Continuous Improvement Report on the DSI Processes.	

Maturity Questions – Data Sharing & Interoperability Domain			
DSI.MQ.2	Has the entity defined and implemented Processes for Sharing Data within the entity and with other Entities?		
Level Name	Level Description	Acceptance Evidence	Related Specification
	- Data-as-a-service (DaaS) and data products are developed and maintained proactively by the entity. - DSI is fully automated and scalable with full control on protection and privacy at the entity level.		

Maturity Questions – Data Sharing & Interoperability Domain			
DSI.MQ.3	Has the entity defined and implemented a data integration architecture to manage the data movement efficiently across data stores, systems, and applications?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No practices in place to manage the data movement across the entity's systems and applications.	- No required documents	
Level 1: Establishing	- Data movement across data stores, systems, and applications is performed on a reactive or ad-hoc basis as needed, with no formal architecture (structure).	- Evidences of Data Movement / Integration within the Entity and with Other Entities.	
Level 2: Defined	- The entity defines its business requirements for each initiative requiring data integration between Data stores, systems, and applications. - The entity develops a solution design document for each data integration initiative based on the target data integration architecture and the Integration Requirements Document.	- The Integration Requirements Document.	- DSI.3.1
		- The Solution Design Document.	- DSI.3.2
Level 3: Activated	- The entity is implementing the data integration architecture following an integration solution development lifecycle for each data integration initiative. - The entity performs testing of the developed integration solution before deployment to the production environment. - - Data sources are integrated through established and approved integration patterns.	All level 2 acceptance evidence requirements including: - The Document of the Approved Standardized Entity Wide Integration Solution Development Lifecycle.	
		- The Developed Test Scripts and the Conducted Tests (Integration, Functional) in	- DSI.3.3

Maturity Questions – Data Sharing & Interoperability Domain			
DSI.MQ.3	Has the entity defined and implemented a data integration architecture to manage the data movement efficiently across data stores, systems, and applications?		
Level Name	Level Description	Acceptance Evidence	Related Specification
		Line with the Plan and the Solution Design Document.	
Level 4: Managed	- The entity is monitoring the effectiveness of the integration initiatives with pre-defined KPIs.	All level 3 acceptance evidence requirements including: - The Monitoring Report with Pre-defined KPIs for the Data Integration Initiatives.	- DSI.8.1 (1,2)
		- The Integration Solution Monitoring and Maintenance Document.	- DSI.3.4
Level 5: Pioneer	- The entity reviews the integration architecture regularly and optimizes the integrations practices by adopting cutting edge methodologies (e.g., Implementing Continuous Integration and Continuous Deployment (CI/CD) pipelines) to automate and streamline the improvement of the integration solution.	All level 4 acceptance evidence requirements including: - The Continuous Improvement Report on the Data Integration Practices.	
		- The Continuous Improvement Mechanisms for Data Integration, e.g.: Continuous Integration & Continuous Delivery (CI/CD) Pipeline Details for Automation.	

Maturity Questions – Data Sharing & Interoperability Domain			
DSI.MQ.4	Has the entity developed and implemented Data Sharing Controls and Processes for efficient data transformation and movement?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No controls or processes in place for data sharing or data transformation and movement.	- No required documents	

Maturity Questions – Data Sharing & Interoperability Domain			
DSI.MQ.4	Has the entity developed and implemented Data Sharing Controls and Processes for efficient data transformation and movement?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 1: Establishing	The entity implements controls for data sharing and movement across applications on a reactive or ad-hoc basis as needed, with no formal controls or processes.	The Existing Data Integration or Data Movement Processes within the Entity.	
Level 2: Defined	- The entity has defined data sharing controls, processes and standards for data transformation and data movement across the entity's applications. - The entity has conducted a risk assessment of DSI processes. - The entity has defined specific processes to classify, protect and support data privacy.	The Developed Data Migration Processes (i.e.: ETL).	- DSI.4.1
		The Developed Data Migration Processes (i.e.: ETL).	- DSI.4.2
		The Risk Assessment Report on the Entity's Datasets to be Shared.	
		The Defined Data Sharing Controls.	
Level 3: Activated	- The entity is implementing defined processes for data transformation and movement (ETL/ELT), and controls for Data Sharing. This includes processes for integrating data from disparate sources and loading into Data Warehouse Store, and processes for storing unstructured data in its raw native format in the Data Lake. - The entity is implementing standards for data development, transformation and movement across all applications. - The data security controls are implemented in line with the security controls published by the KSA's National Cybersecurity Authority (NCA). - Appropriate controls are applied on the datasets to be shared in line with the Data Sharing regulations and other relevant regulations (e.g., Personal Data Protection (PDP) etc.).	All level 2 acceptance evidence requirements including: A Report on the Implemented Controls (e.g.: Data Security & Protection, Data Sharing, Data Integration, Data Access, etc.).	
		Evidence of the Implemented Data Migration Processes (i.e.: "Extract, Transform, Load (ETL)).	- DSI.4.1
		Evidence of the Implemented Data Migration Processes (i.e.: "Extract, Load, Transform (ELT)).	- DSI.4.2
Level 4: Managed	The entity is monitoring the effectiveness of the DSI controls, processes and standards with pre-defined KPIs.	All level 3 acceptance evidence requirements including: The Monitoring Report with Pre-defined KPIs for the DSI Controls, Processes and Standards.	
Level 5: Pioneer	- The entity continuously reviews its data sharing and integration controls and practices for optimization by adopting advanced interoperability standards (e.g., Event driven, event sourcing, data mesh, etc.). - The transformed and merged data is available upon request as a service (DaaS) for various transactions, reporting and analysis in	All level 4 acceptance evidence requirements including: The Continuous Improvement Report on Reviewing the DSI Processes and Mechanisms to Automate the DSI Controls and Practices.	

Maturity Questions – Data Sharing & Interoperability Domain			
DSI.MQ.4	Has the entity developed and implemented Data Sharing Controls and Processes for efficient data transformation and movement?		
Level Name	Level Description	Acceptance Evidence	Related Specification
	the entity for innovation (e.g., data-driven transformation and products, etc.). - Proactive periodic audits and reviews of the applications and systems are performed in an automated way.		

8.1.8.Reference and Master Data Management Domain

Maturity Questions – Reference and Master Data Management Domain			
RMD.MQ.1	Has the entity developed and implemented a plan focused on improving its Reference & Master Data (RMD) Management capabilities?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- The entity doesn't have a plan in place for Reference & Master Data (RMD) Management.	- No required documents	
Level 1: Establishing	- The entity manages its Reference & Master Data (RMD) on a reactive or ad-hoc basis with no formalized practices.	- The Currently Existing Practices Related to the RMD Management Domain.	
Level 2: Defined	- The entity has a defined and approved RMD Management plan. - A roadmap is defined with a list of activities, required resources, trainings and a budget to manage the RMD plan implementation.	- The Developed and Approved RMD Management Plan.	- RMD.1.1
Level 3: Activated	- The entity is implementing the defined RMD Management plan and roadmap. - Clear roles and responsibilities are defined and activated for the RMD activities. - Business and IT data stewards are assigned in line with the "Data Management Organization" structure. - The entity trains all employees responsible for the management of its RMD as required in line with the change management practices.	All level 2 acceptance evidence requirements including: - The RMD Management Plan Implementation Status Report.	
		- The RMD Management Training Implementation Status Report.	- RMD.3.1
		- The RMD Management Operating Model Showing the RMD Stewardship Coverage.	- RMD.4.1

Maturity Questions – Reference and Master Data Management Domain			
RMD.MQ.1	Has the entity developed and implemented a plan focused on improving its Reference & Master Data (RMD) Management capabilities?		
Level Name	Level Description	Acceptance Evidence	Related Specification
	- The RMD change request logs and the decisions are documented.	- The RMD Change Request Logs.	- RMD.6.1
	- Documented and registered RMD Management initiatives are being implemented in the statement of Architecture work.	- The RMD Management Documents & Artifacts.	- RMD.6.2
Level 4: Managed	- The entity is monitoring the effectiveness of the RMD Management plan and activities with pre-defined KPIs.	All level 3 acceptance Evidence requirements, Including: - The Monitoring Report of the RMD Management Plan Implementation with Pre-defined KPIs.	
Level 5: Pioneer	- The entity's RMD Management plan and activities are continuously reviewed and updated for optimization and improvement.	All level 4 acceptance Evidence requirements, Including: - The Continuous Improvement Report of the RMD Management Plan.	

Maturity Questions – Reference and Master Data Management Domain			
RMD.MQ.2	Has the entity defined and implemented processes to manage its Reference & Master Data (RMD) objects from creation to archival?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No processes are in place for Reference & Master Data (RMD) management.	- No required documents	
Level 1: Establishing	- The entity implements Reference and Master Data Management Operations as needed on a reactive basis or partially for certain projects/initiatives with no formalized practices.	- Evidence of Projects / Initiatives with Reference Data and/or Master Data Identified.	
Level 2: Defined	- The entity has defined processes to manage its RMD objects across the business and technical applications. - RMD requirements are documented in line with business needs. - RMD objects are identified, prioritized, and categorized (Internal or External). - Standards and rules for matching and merging Master Data Objects and Reference Datasets are defined.	- The Identified, Prioritized and Categorized RMD Objects.	- RMD.1.2
		- Reference Data Categorization.	- RMD.1.3
		- Master Data Categorization.	- RMD.1.4
		- The Reference & Master Data Requirements.	- RMD.2.1

Maturity Questions – Reference and Master Data Management Domain			
RMD.MQ.2	Has the entity defined and implemented processes to manage its Reference & Master Data (RMD) objects from creation to archival?		
Level Name	Level Description	Acceptance Evidence	Related Specification
	- Processes are developed for the RMD lifecycle (Creation, modification, and archiving). - Service Level Agreements (SLAs) are defined for the processes.	- The Defined SLAs for RMD Lifecycle Management.	- RMD.5.1
Level 3: Activated	- The entity is implementing its RMD Management Processes. - Match and Merge, survivorship rules for Reference Data Objects are embedded in the data transformation rules and implemented on the entity's data applications. - Rules for standardized Reference data are embedded in the entity's data applications and managed centrally, considering the use of national reference data.	All level 2 acceptance evidence requirements including: - The RMD Lifecycle Management Process	- RMD.4.2
		- Evidence of the entity's participation in or use of national reference datasets.	
Level 4: Managed	- The entity is monitoring the processes for managing the RMD Objects across the data lifecycle with pre-defined KPIs.	All level 3 acceptance Evidence requirements, Including: - The Monitoring Report of the RMD Management Processes with Pre-defined KPIs & SLAs.	- RMD.5.2
Level 5: Pioneer	- The entity's RMD Management Processes and Standards are continuously monitored for optimization and improvement.	All level 4 acceptance Evidence requirements, Including: - The Continuous Improvement Report of the RMD Management Processes & Standards.	

Maturity Questions – Reference and Master Data Management Domain			
RMD.MQ.3	Has the entity implemented a Data Hub (or Tool) as the trusted data source to support the RMD Management Processes?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No tools are in place for managing the Reference & Master Data (RMD).	- No required documents	
Level 1: Establishing	- The entity manages its RMD within standalone data sources without standardized tools.	- Evidence that the entity manages its RMD within standalone data sources without standardized tools.	
Level 2: Defined	- The entity identified the required Hub / Tool for RMD Management based on business and technical requirements. - A suitable Data Hub architecture implementation pattern is agreed upon and the Data Hub design is developed. - A conceptual and information architecture is developed based on the selected Data Hub Architecture Design. - RMD models and architectures are developed. - RMD Hub / Tool technical requirements are documented based on the defined target RMD information Architecture.	- The Target RMD Management Architecture Design.	- RMD.2.2
		- The Developed RMD Conceptual Architecture.	- RMD.2.3
		- The Developed RMD Information Architecture.	- RMD.2.4
		- The RMD Hub / Tool Technical Requirements.	- RMD.2.5
Level 3: Activated	- The entity implemented the selected Data Hub for RMD Management and is operating the hub as the Trusted Source of RMD across the entity. - The implemented Data Hub is flexible to accommodate new data sources and to support workflow capabilities and customizations (e.g., data localization, privacy, consent management, hierarchy management, and exception processing and automated alert capabilities).	All level 2 acceptance Evidence requirements, Including: - The Implemented RMD Management Hub.	- RMD.4.3

Maturity Questions – Reference and Master Data Management Domain			
RMD.MQ.3	Has the entity implemented a Data Hub (or Tool) as the trusted data source to support the RMD Management Processes?		
Level Name	Level Description	Acceptance Evidence	Related Specification
		- The Workflow Documentation Showing the Establishment of the Data Hub as the Entity's Trusted Source.	- RMD.4.4
Level 4: Managed	- The entity is monitoring the adoption and usage of the implemented Data Hub with the pre-defined KPIs.	All level 3 acceptance Evidence requirements, Including: - The Monitoring Report of the RMD Management Hub / Tool Capabilities with Pre-defined Key Performance Indicators (KPIs).	
Level 5: Pioneer	- The entity continuously inspects the implemented Data Hub to: • Ensure full coverage of all new and updated data sources. • Ensure that all deployed tools and technologies are regularly optimized. • Ensure that the level of automation increased based on industry and global trends. - A centralized Hub / Tool is developed being the Trusted Data Source wherein all the RMD Objects are hosted and maintained.	All level 4 acceptance evidence requirements, Including: - The Continuous Improvement Report of the RMD Information Architecture and the Implemented Data Hub.	

8.1.9. Business Intelligence and Analytics Domain

Maturity Questions – Business Intelligence and Analytics Domain			
BIA.MQ.1	Has the entity developed and implemented a plan to manage and orchestrate its Business Intelligence & Analytics (BIA) activities?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	No formal Business Intelligence & Analytics (BIA) plan is in place.	No required documents	
Level 1: Establishing	The entity implements BIA activities as needed, on a reactive or ad-hoc basis.	Current activities related to BIA.	
Level 2: Defined	- The entity has a defined and approved BIA plan based on the overall Data Management (DM) strategy. - A roadmap is defined with a list of activities, required resources and budget to manage the BIA implementation.	The defined & approved BIA Plan.	- BIA.1.1
Level 3: Activated	- The entity is implementing the defined & approved BIA plan & roadmap. - Clear roles and responsibilities are defined for the BIA activities in line with the Data Management Organization structure.	All level 2 acceptance evidence requirements including: The BIA plan & roadmap implementation status report.	
		The Defined & Documented Roles & Responsibilities for BIA Activities Including Data Stewardship Roles.	
Level 4: Managed	The entity is monitoring the effectiveness of the BIA plan and activities with pre-defined Key Performance Indicators (KPIs).	All level 3 acceptance evidence requirements including: The Effectiveness Monitoring Report of the BIA plan & activities according to the pre-defined Key Performance Indicators (KPIs).	
Level 5: Pioneer	The BIA plan and activities are continuously reviewed and updated for optimization and improvement.	All level 4 acceptance evidence requirements including: Regular reviews and improvements to the business intelligence and analytics plan and roadmap.	

Maturity Questions – Business Intelligence and Analytics Domain			
BIA.MQ.2	Has the entity identified BIA use cases and defined a plan for the use case implementation?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	No defined BIA use cases are identified within the entity.	No required documents	
Level 1: Establishing	The entity identifies and implements BIA use cases on ad hoc basis or for specific projects and initiatives.	List of the implemented BIA uses cases within the Entity.	
Level 2: Defined	- The entity has identified and prioritized its BIA use cases using a defined prioritization framework. - Shortlisted use cases have been documented in a detailed BIA Use Case Portfolio document. - An Implementation plan has been developed for each shortlisted and approved use case with implementation priorities based on the entity's defined use case implementation approach. - A use case validation process has been developed.	The approved BIA business cases / BIA use cases.	
		The approved BIA Use Cases Prioritization Framework.	- BIA.1.2
		The shortlisted / prioritized use cases based on business needs.	- BIA.1.2
		The BIA Use Case Portfolio document with details of each use case.	- BIA.1.3
		The Approved Use Case implementation plan.	- BIA.1.4
		The defined use case implementation approach (e.g., DevOps, Agile, etc.).	
		The approved use case validation process.	- BIA.3.1
Level 3: Activated	- The entity is implementing and validating the prioritized use cases in order to transform the entity into a data-driven organization. - The new use cases are evaluated and implemented based on the business requirements. - The Implemented BIA use cases and their final outcomes are documented in a register.	All level 2 acceptance evidence requirements including: The Implemented and new Use Cases.	
		The up-to-date BIA use cases register.	- BIA.5.1
		The Outcomes of the BIA Use Case Validation Processes.	
Level 4: Managed	- The entity is evaluating / monitoring the performance of analytical models and business impacts of implemented use cases with pre-defined Key Performance Indicators (KPIs). - The Technical or Business impacts and the Return on Investment (ROI) from the use cases are monitored with pre-defined KPIs.	All level 3 acceptance evidence requirements including: The Monitoring Report on the BIA Portfolio Effectiveness with pre-defined Key Performance Indicators (KPIs).	- BIA.4.1

Maturity Questions – Business Intelligence and Analytics Domain			
BIA.MQ.2	Has the entity identified BIA use cases and defined a plan for the use case implementation?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 5: Pioneer	- The entity's activated and implemented BIA use cases are regularly reviewed and optimized. - The potential impact, competitive advantage, Total Cost of Ownership (TCO) and Return on Investment (ROI) are continuously reviewed and updated with a defined calculation methodology.	All level 4 acceptance evidence requirements including: - The Continuous Improvement Report on BIA Use Cases.	
		- The Updated BIA Use Case Register and the Optimized Use Cases.	

Maturity Questions – Business Intelligence and Analytics Domain			
BIA.MQ.3	Has the entity defined and implemented practices to manage and govern the BIA processes?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No practices are in place for BIA.	- No required documents	
Level 1: Establishing	- The entity manages its BIA processes as needed, on a reactive or ad-hoc basis without formalized practices. - Reporting is done either on direct source systems; or different Data Marts are developed based on the business needs with no semantic relationship / link among them. - The BIA Governance focuses only on the requirements of the projects. - The DQ issues are resolved during the data population for BI by the BI team.	- The Existing BIA Domain Processes & Governance Documentation.	
		- The List of Existing Reports & Dashboards.	
Level 2: Defined	- The entity has defined formal BIA practices including the development of processes for a data warehouse or a Data Lake with logical models in place to model the business functions. - A Semantic layer is developed and maintained for supporting BI and Advanced Analytics use cases. - The entity is developing a change management plan including training programs, awareness campaigns and a release management process to guide the publishing mechanism of reports, dashboards and implemented uses cases.	- The Developed & Approved Processes of BIA Management.	
		- The Approved Process of New Data Source Requirements.	
		- The Approved Demand Management Process.	
		- Development and maintenance document of the Semantic Layer.	
		- Advanced analytics management and governance process.	
		- The identified & developed Data Sources & Data Marts.	

Maturity Questions – Business Intelligence and Analytics Domain			
BIA.MQ.3	Has the entity defined and implemented practices to manage and govern the BIA processes?		
Level Name	Level Description	Acceptance Evidence	Related Specification
		- The Developed & Approved Change Management Plan including The training programs.	- BIA.2.1
		- The Developed & Approved Change Management Plan including Awareness campaigns.	- BIA.2.2
Level 3: Activated	- The entity is implementing the defined BIA processes and practices which are established to govern BIA activities. - Self-service analytics are fully activated covering both BI and Artificial Intelligence / Machine Learning (AI/ML). - Business users have full access to all types of data (Raw, Processed, Modelled) in a governed manner. - End-to-end governance is in place covering emerging topics such as AI ethics, etc. - Advanced Analytics (AI/ML) governance and management (AI/ML OPs) foundational processes are in place operationally. - A central Data Science & BIA team has been set up with defined roles and responsibilities. - The central Data Science & BIA team has a clear process flow to handle the entity's BIA needs. - BIA training courses are conducted for all employees involved in the BIA initiatives to upskill the analytics capabilities; and awareness campaigns are conducted to promote the awareness, education & adoption of the BIA capabilities.	All level 2 acceptance evidence requirements including:	
		- Evidences of the adoption & implementation for business intelligence and analytics management and governance.	
		- The approved Operating Model with defined roles & responsibilities for The Data Science team.	- BIA.3.2
		- Evidences of training courses & awareness campaigns conducted.	
		- The approved User Acceptance Test (UAT) Documents.	
		- The approved outcomes as Reports & Dashboards produced for The Business Units.	
		- The Capacity planning document.	
Level 4: Managed	- The entity is monitoring BIA processes, governance and the performance of the centralized BI team with pre-defined Key Performance Indicators (KPIs).	All level 3 acceptance evidence requirements including: - The Monitoring Report on the effectiveness of practices and processes for managing and governing business intelligence and analytics through pre-defined Key Performance Indicators (KPIs).	

Maturity Questions – Business Intelligence and Analytics Domain			
BIA.MQ.3	Has the entity defined and implemented practices to manage and govern the BIA processes?		
Level Name	Level Description	Acceptance Evidence	Related Specification
		- The monitoring Report on the effectiveness of training and awareness sessions conducted through pre-defined Key Performance Indicators (KPIs).	- BIA.4.1
		- Performance Measurement Report for the Business Intelligence and Analytics Team.	
Level 5: Pioneer	- The entity created a BI Competency center including the required roles, skills & capabilities to fulfil all BI requirements. - The entity created a BI Competency center which governs the entity's BI management including the demand management and change management. - The performance of the BIA team is continuously reviewed, measured and optimized. - The BIA Capacity planning is reviewed regularly and fulfilled to support the growing demand.	All level 4 acceptance evidence requirements including:	
		- Establishment of Business Intelligence and Analytics Center Document.	
		- The continuous review and improvement of business intelligence and analytics management and governance practices.	
		- The continuous Review and Improvement of Business Intelligence and Analytics Team Performance.	
		- The Updated Capacity Planning document.	
		- The Revised Demand Management Process.	

Maturity Questions – Business Intelligence and Analytics Domain			
BIA.MQ.4	Has the entity implemented the right tools, technologies, and skills to empower users and support the implementation of the BIA use cases?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No technology for BIA is in place. - The reporting is done manually.	- No required documents	
Level 1: Establishing	- The entity implements its BIA activities on an ad hoc basis or individual applications without formalized tools.	- The list of BIA tools.	
		- The list of reports.	
Level 2: Defined	- The entity selected standardized tools to develop standard analytics artifacts (reports and dashboards). - The Business and IT stakeholders collaborate to develop, enhance and maintain the Semantic Layer.	All Level 1 acceptance evidence requirements including: - The list of business units which use the BIA technology tools.	
Level 3: Activated	- The entity selected and implemented tools and technologies that are currently adopted across the entity. - The entity has self-service advanced analytics (data discovery, wrangling, statistical analysis, etc.) and collaborative Artificial Intelligence / Machine Learning (AI / ML) using a low-code / no-code environment. - Users have the choice of a unified interface in their workflows by using: • Tools. • Programming Languages (e.g., Python, R, Go, etc.). • Platforms (e.g., Anaconda, Jupiter, etc.). • Libraries (e.g., Pandas, Numpy, etc.). - Project documentation is managed centrally and shared across the entity. - Common AI / ML Models are versioned and documented through the tools. - Users have the ability to reuse those AI / ML Models in developing new BI Analytics & Models.	All Level 2 acceptance evidence requirements including: - The list of users with role and privileges.	
		- The Approved Architecture & Documentation for Advanced Analytics.	
		- Advanced Analytics and Communication Project Management Documents.	

Maturity Questions – Business Intelligence and Analytics Domain			
BIA.MQ.4	Has the entity implemented the right tools, technologies, and skills to empower users and support the implementation of the BIA use cases?		
Level Name	Level Description	Acceptance Evidence	Related Specification
		- The Approved Advanced Analytics Models Documents.	
Level 4: Managed	The entity is monitoring the adoption and utilization of the BIA tools and technologies with pre-defined Key Performance Indicators (KPIs).	All Level 3 acceptance evidence requirements including: - Report on the Effectiveness Monitoring of Business Intelligence and Analytics Tools and Techniques through Pre-defined Key Performance Indicators.	
Level 5: Pioneer	New technologies are regularly evaluated, tested, and introduced to keep the capabilities aligned with the future needs. Advanced frameworks are used (e.g., Spark, TensorFlow, PyTorch, etc.) and integrated with their unified AI/ML environment. Advanced capabilities such AI/ML engineering tools and features are used for complex processing and reusability. Tools and technologies which use AI/ML OPs are practiced to manage the end-to-end AI/ML lifecycle.	All Level 4 acceptance evidence requirements including: - Document for Continuous Adoption of Technologies, Tools, Frameworks, and Features.	
		- The Continuous Improvement Report of the BIA and Advanced Analytics Technology Solutions including the Proof of Concept (POC) Roadmap.	
		- A Report on the Proof of Concept (POC) Results.	

8.1.10. Data Value Realization Domain

Maturity Questions – Data Value Realization Domain			
DVR.MQ.1	Has the entity developed a plan to identify, document and realize its data revenue generation potential and implement Data-related cost optimization initiatives and use cases?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No plan is in place to generate value from data nor implement data-related cost optimization initiatives. - No use cases are identified for data revenue generation nor data-related cost optimization.	- No required documents	
Level 1: Establishing	- The entity has existing practices for Data Value Realization (DVR), data-related cost optimization, and identification of use cases, however, it is done as needed, on a reactive or ad-hoc basis without formalized DVR practices.	- The Existing List of Data Value Realization (DVR) Activities.	
Level 2: Defined	- The entity has a defined and approved plan to identify, document and realize value from its data through revenue generation initiatives and data-related cost optimization initiatives. - The entity identified use-cases for revenue generation and cost optimization based on the guidelines for ethical use cases. - The entity estimated and projected a Payback period and Return on Investment (ROI) for each identified use case. - Roles and responsibilities to support the DVR implementation have been identified and documented.	- The Data Value Realization (DVR) plan.	- DVR.1.2
		- The List of Identified Use Cases for Both Revenue Generation & Cost Optimization.	- DVR.1.1
		- A Document Explaining the Payback Period and Return on Investment (ROI) for Each Identified Use Case.	- DVR.1.1
Level 3: Activated	- The entity is implementing its DVR plan through use-cases for revenue generation and cost optimization. - Roles and responsibilities for DVR use-case implementations are activated in line with the Data Management Organization structure. - The entity is maintaining the DVR use cases.	All level 2 acceptance Evidence requirements, Including: - Report on DVR Monitoring & Maintenance.	- DVR.3.1
		- Implementation plan status report of Data Value Realization (DVR).	
		- The Organizational Structure for Data Value Realization (DVR) Activities.	
Level 4: Managed	- The entity is monitoring the efficiency of the plan implementation and DVR activities with pre-defined Key Performance Indicators (KPIs) in line with the “DM and PDP Standards” document.	All level 3 acceptance Evidence requirements, Including: - The Monitoring Report of the DVR use cases with pre-defined KPIs.	- DVR.4.1 (1, 2, 6, 7)

Maturity Questions – Data Value Realization Domain			
DVR.MQ.1	Has the entity developed a plan to identify, document and realize its data revenue generation potential and implement Data-related cost optimization initiatives and use cases?		
Level Name	Level Description	Acceptance Evidence	Related Specification
		- The Monitoring Report of the DVR Activities & Plan with Pre-defined KPIs.	
Level 5: Pioneer	- The DVR plan implementation is regularly reviewed and optimized to ensure continuous improvement.	All level 4 acceptance evidence including: - Review & Continuous Improvement Document of the DVR Plan.	
		- The Revised & Updated DVR KPIs.	
		- Evidences of New Partnerships (e.g., MoU, jointly developed use cases or products, etc.).	

Maturity Questions – Data Value Realization Domain			
DVR.MQ.2	Has the entity implemented practices to support a Data revenue generation process?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No processes are in place for use cases of both: data revenue generation and cost optimization.	- No required documents	
Level 1: Establishing	- The entity has not implemented a formalized process for data revenue generation, however, it is done as needed, in a reactive or ad-hoc basis.	- The Existing Practices Related to Supporting the Data Revenue Generation Process.	
Level 2: Defined	- The entity has a defined, documented, and approved process for data revenue generation covering the details of: • The selection of a pricing schema model. • The calculation of the total cost. • Aligning the adopted charging model in line with the business needs.	- The Defined Pricing Scheme.	- DVR.2.1
		- The Data or Data Product Price Calculation.	- DVR.2.2

Maturity Questions – Data Value Realization Domain			
DVR.MQ.2	Has the entity implemented practices to support a Data revenue generation process?		
Level Name	Level Description	Acceptance Evidence	Related Specification
		- The Adopted / Approved Charging Model for Each Data or Data Product.	- DVR.2.3
Level 3: Activated	- The entity is implementing the defined process of data revenue generation. - For each data revenue generation request, the entity submits the required documentation to the internal DMO. - For each data or data product that the entity is expecting to generate revenue from, the entity submits a revenue generation request to the internal DMO.	All level 2 acceptance evidence including: - Evidences of Revenue Generation Requests Submitted to the internal DMO at the entity.	- DVR.2.4
Level 4: Managed	- The entity is monitoring the efficiency of the data revenue generation process with pre-defined KPIs.	All level 3 acceptance evidence including: - The Monitoring Report of the Data Revenue Generation Process with Pre-defined KPIs.	- DVR.4.1 (3,4,5)
Level 5: Pioneer	- The Revenue Generation Process is regularly reviewed and optimized to ensure continuous improvement.	All level 4 acceptance evidence including: - The Continuous Improvement Report of the Data Revenue Generation Process.	

8.1.11. Open Data Domain

Maturity Questions – Open Data Domain			
OD.MQ.1	Has the entity defined, established, and implemented a plan to identify and coordinate the publishing of its Open Datasets?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	No Open Data (OD) plan is in place.	No required documents	
Level 1: Establishing	The entity has existing practices related to OD, but these practices are not formalized.	The existing list of Open Datasets.	
Level 2: Defined	- The entity has defined an OD plan and framework. - OD Management structure is in place and a change management plan has been developed to conduct training on OD activities and awareness campaigns.	The approved Open Data Framework.	
		The approved Open Data plan.	OD.1.1
		The OD Management structure.	
		The developed and approved plan for change management including: Awareness campaigns.	OD.2.1
Level 3: Activated	- The entity is implementing the activities on the defined Open Data plan including training & awareness programs. - An annual report on the Open Data plan & progress is submitted to NDMO-SDAIA. - The entity appointed the following roles in line with the Data Management Organization: - Open Data & Information Access Officer (ODIAO) to lead the Open Data activities within the entity. - Business Data Executive (BDE). - Business Data Steward.	- All level 2 acceptance evidence requirements including: - The Open Data Plan Implementation status report.	
		Evidence of submission of the annual Compliance report to NDMO-SDAIA.	
		Assignment decisions / appointees to job roles.	
		Evidence of Implementation of the Change Management Program (The conducted training courses and the launched awareness campaigns related to Open Data).	

Maturity Questions – Open Data Domain			
OD.MQ.1	Has the entity defined, established, and implemented a plan to identify and coordinate the publishing of its Open Datasets?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 4: Managed	- The entity is monitoring the effectiveness of the Open Data activities plan with pre-defined Key Performance Indicators (KPIs).	All level 3 acceptance evidence requirements including: - The Monitoring Report on the Effectiveness of the Open Data Plan through Pre-defined Key Performance Indicators (KPIs).	- OD.4.1
Level 5: Pioneer	- The Open Data plan is revised & optimized for continuous improvement.	All level 4 acceptance evidence requirements including: - The periodic reviews and improvements of the open data plan.	

Maturity Questions – Open Data Domain

OD.MQ.2	Has the entity defined, established, and implemented a process to support the Identification of Open Data (OD)?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No existing process is in place to identify Open Data (OD) within the entity.	- No required documents	
Level 1: Establishing	- Open Data identification practices are performed on a reactive or ad hoc basis, without formalized OD practices.	- The Existing Practices for OD Identification.	
Level 2: Defined	- The entity has developed and documented processes required to manage the lifecycle of Open Data. - In alignment with the Open Data Policy, the entity defined a process to identify public datasets to be published including a mechanism to evaluate all data classified as "Public Data" to determine whether to be published as OD or not.	- The Defined Process Documentation for managing the lifecycle of Open Data.	- OD.3.1
		- The Defined Process Documentation for Identifying Open Data.	
		- The process of evaluating the value and impact of open or public datasets.	
Level 3: Activated	- The entity is implementing the defined processes for identifying the datasets to be published. - The entity is evaluating the identified datasets in terms of value whilst also conducting risk assessment to ensure there will be no security or privacy threats when published. - The Identified Open Datasets are being aligned with the regulations published by NDMO-SDAIA. - The entity has identified & documented metadata of the entity's open datasets.	All level 2 acceptance evidence requirements including:	
		- The OD Identification Process Implementation Status Report.	
		- The list of Identified Open Datasets with the assigned priorities.	- OD.3.2
		- The Identified & Documented Metadata for the Open Datasets.	- OD.3.4
Level 4: Managed	- The entity is monitoring the effectiveness of the implemented processes of identifying Open Datasets with pre-defined KPIs.	- Value and Impact Assessment Report for Identified Open or Public Datasets.	- OD.3.2
		All level 3 acceptance evidence including:	- OD.4.1 (KPI 2)
		- The Monitoring Report of OD Identification & Prioritization Processes with Pre-defined KPIs.	

Maturity Questions – Open Data Domain			
OD.MQ.2	Has the entity defined, established, and implemented a process to support the identification of Open Data (OD)?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 5: Pioneer	The entity is conducting continuous improvement, enabled by automated processes to support OD identification.	All level 4 acceptance evidence requirements including: The Continuous Improvement Report Showing the Documented Periodic Reviews & Outcomes of the OD Identification Processes and the Implemented Automation.	

Maturity Questions – Open Data Domain			
OD.MQ.3	Has the entity defined, established, and implemented a process to support publishing its Open Datasets?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	No existing processes are in place to support the publishing of Open Datasets.	No required documents	
Level 1: Establishing	Open Data (OD) is published as needed, on a reactive or ad-hoc basis.	The Existing Practices for Publishing Open Datasets.	
Level 2: Defined	- The entity has defined a process to manage the publishing of Open Datasets as part of the documented Open Data processes. - The entity has defined a process to regularly review, update and document changes to its published Open Datasets and associated metadata to ensure they meet defined regulatory requirements.	The Defined Process Documentation for Publishing Open Data.	
		The Defined Process Documentation for Open Data Maintenance.	
Level 3: Activated	The entity is implementing the defined process for publishing Open Data by collaborating with National Information Center (NIC) in SDAIA to publish the Open Datasets on the Saudi Open Data Platform under the KSA Open Data License.	All level 2 acceptance evidence requirements including: Status Report on the Implementation of the Open Data Publishing Process.	

Maturity Questions – Open Data Domain

OD.MQ.3	Has the entity defined, established, and implemented a process to support publishing its Open Datasets?		
Level Name	Level Description	Acceptance Evidence	Related Specification
	- The entity utilizes standardized formats when publishing its datasets that are in machine-readable form. - The entity ensures that the open datasets are published in high quality to ensure fitness for use. - The entity is updating the published open datasets and the associated Metadata and maintaining data traceability and versioning history of the open datasets. - The entity is documenting in a register its identified open datasets and activities.	- Evidences of Published Datasets on the Saudi Open Data Platform.	- OD.3.3
		- Evidences of Feedback / Comments Received on OD.	
		- Evidence of formats used to standardize open datasets in machine readable form.	- OD.3.5
		- Evidence of data standards applied on open datasets to ensure high data quality.	
		- Open Data Maintenance Report.	- OD.3.6
		- Open Data Register containing Records of Open Data Activities and Published Open Datasets.	- OD.5.1
Level 4: Managed	- The entity is monitoring the effectiveness of the Open Data processes with pre-defined KPIs, covering: 1. The number of downloads per published Open Dataset. 2. The number of defined, identified and prioritized Open Datasets. 3. The number of identified Open Datasets that have been published. 4. The number of updates performed on published Open Datasets.	All level 3 acceptance evidence requirements including: - The Monitoring Report of the OD Publishing Process with Pre-defined KPIs.	- OD.4.1 (KPIs: 1, 3, 4)
Level 5: Pioneer	- The entity is conducting continuous improvement to support the defined OD publishing processes to ensure optimization. - The published Open Datasets and the associated Metadata are regularly reviewed and updated to the newest version. - The OD and the associated Metadata changes are documented where necessary.	All level 4 acceptance evidence requirements including: - The Continuous Improvement Report of the OD Publication & Maintenance Practices and Outcomes.	

8.1.12. Freedom of Information Domain

Maturity Questions – Freedom of Information Domain			
FOI.MQ.1	Has the entity defined and established a plan to address its compliance with the requirements of the Freedom of Information (FOI) Regulations?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	No plan is in place to address the Freedom of Information (FOI) regulations within the entity.	No required documents	
Level 1: Establishing	The entity has existing FOI practices in place to address its compliance with the FOI Regulations without formalized practices.	The Existing FOI Practices.	
Level 2: Defined	- The entity has a defined and approved FOI plan. - A roadmap is defined with a list of activities, required resources, training courses & awareness campaigns, and a budget to manage the FOI plan implementation.	The Defined & Approved FOI Implementation Plan & Roadmap.	FOI.1.1
Level 3: Activated	- The entity is implementing the (pre) defined plan to manage FOI requests. - The entity is publishing on its official Government website with a feedback mechanism for questions or issues raised. - The entity appointed an Open Data & Information Access Officer (ODIAO) to manage the entity's compliance with the FOI regulations in line with the "Data Management Organization" structure. - The entity launched awareness campaigns to promote and enhance the culture of transparency and to raise awareness of the FOI regulations published by NDMO-SDAIA.	All level 2 Acceptance Evidence requirements, Including: The FOI Plan Implementation Status Report.	
		The Assigned Open Data & Information Access Officer (ODIAO).	
		FOI Awareness.	FOI.2.1
Level 4: Managed	- To comply with the FOI Regulations, the entity is monitoring the effectiveness of the plan established with pre-defined Key Performance Indicators (KPIs). - The entity is conducting periodic audit and review processes on the compliance with FOI regulations published by NDMO-SDAIA.	All level 3 Acceptance Evidence requirements, Including: The Monitoring Report on the Entity's FOI Plan & Activities with Pre-defined Key Performance Indicators (KPIs).	
		The Internal audit reports on the entity's Compliance with the FOI Regulations.	FOI.3.6

Maturity Questions – Freedom of Information Domain			
FOI.MQ.1	Has the entity defined and established a plan to address its compliance with the requirements of the Freedom of Information (FOI) Regulations?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 5: Pioneer	- The entity's FOI plans and practices are continuously reviewed and optimized.	All level 4 Acceptance Evidences required, Including: - The Continuous Improvement Report of the FOI Plan.	

Maturity Questions – Freedom of Information Domain			
FOI.MQ.2	Has the entity defined and implemented the required processes for Freedom of Information (FOI)?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No existing practices are in place for Freedom of Information (FOI) within the entity.	- No required documents	
Level 1: Establishing	- The entity responds to FOI requests on a reactive and ad hoc basis.	- The Existing Processes for the FOI Requests & Responses.	
Level 2: Defined	- The entity has defined processes to manage FOI requests (including response processes and appeal / denial processes) in alignment with the National Data Governance Regulations. - The entity has developed end-to-end processes, steps and Frequently Asked questions (FAQs) for acquiring information from the official Gov portal / website.	- The Developed & Approved FOI Request Processes & Procedures Documentation.	- FOI.3.1
		- The Developed FOI Process Guide & FAQs.	
Level 3: Activated	- The entity is implementing the defined processes and practices for FOI Regulatory Compliance to ensure adoption across the entity. - The entity is publishing on the official portal / website, the end-to-end process guide and the FAQs required for acquiring the information. - An FOI Request Management process is activated across the entity, including access and appeal / denial practices.	All level 2 Acceptance Evidences required including: - The Implementation / Adoption Status Report on the FOI Request Processes.	- FOI.3.2
		- Evidences of Entity-wide Communication	- FOI.3.3
		- The Register of the Received Request Forms with the Responses.	- FOI.3.4

Maturity Questions – Freedom of Information Domain

FOI.MQ.2	Has the entity defined and implemented the required processes for Freedom of Information (FOI)?		
Level Name	Level Description	Acceptance Evidence	Related Specification
	- The entity has a record keeping system which is regularly updated on the FOI Register. - The entity adopted a pricing scheme for Public Information Access Requests.	- The Identified Public Datasets Shared Under the FOI Regulations.	
		- Evidences of the Published FOI Communications.	- FOI.3.3
		- The Pricing Scheme for Public Information Access Requests.	- FOI.3.5
		- The Up-to-date FOI Register.	- FOI.4.1
Level 4: Managed	- The entity is monitoring the completeness and performance of the FOI processes with pre-defined KPIs.	All level 3 Acceptance Evidence requirements, Including: - The Monitoring Report with Pre-defined KPIs for the Entity's Responses on FOI Requests.	
Level 5: Pioneer	- The entity continuously reviews & optimizes FOI processes & practices. - The FOI request responding process is automated.	All level 4 Acceptance Evidence requirements, Including: - The Continuous Improvement Report on the FOI Processes.	
		- The Automated tool for FOI requests.	

8.1.13. Data Classification Domain

Maturity Questions – Data Classification Domain			
DC.MQ.1	Has the entity established a plan for Data Classification (DC) as stipulated by the Data Management and personal data protection (DM & PDP) standards?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No plan for Data Classification (DC) is in place.	- No required documents	
Level 1: Establishing	- The entity manages DC practices as needed, on a reactive and ad-hoc basis, with no formalized practices.	- The Existing DC Practices.	
Level 2: Defined	- The entity defined a plan for DC to manage and orchestrate its DC activities.	- The defined & Approved Data Classification Plan.	- DC.1.1
Level 3: Activated	- The entity has implemented the defined DC plan and roadmap on all approved datasets/artifacts.	All level 2 acceptance evidence requirements including: - The Data Classification implementation plan status report.	
Level 4: Managed	- The entity is monitoring the effectiveness of the DC plan & activities with the pre-defined Key Performance Indicators (KPIs).	All level 3 acceptance evidence requirements including: - The Implementation Monitoring Report of the DC Plan & Activities with Pre-defined KPIs.	
Level 5: Pioneer	- The DC plan & activities are continuously reviewed & updated for optimization & improvement.	All level 4 acceptance evidence requirements including: - Data classification plan review report.	

Maturity Questions – Data Classification Domain			
DC.MQ.2	Has the entity defined, identified and implemented the required Data Classification (DC) processes?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	No existing processes for Data Classification (DC) are in place within the entity.	No required documents	
Level 1: Establishing	Existing DC activities are performed on a reactive or ad hoc basis.	The Current List of Classified Datasets.	
Level 2: Defined	- The entity developed a prioritization framework to classify its datasets. - The entity developed a framework for conducting the impact assessment. - The entity defined data handling data protection Controls for the datasets and artifacts. - The entity defined & identified the DC levels based on NDMO-SDAIA standards. - The entity defined a process for identification and inventory of its datasets and artifacts	Data Classification Policy.	
		The Data Handling and Protection Controls.	DC.2.1
Level 3: Activated	- The entity is identifying and maintaining an inventory of all datasets and artifacts owned by the entity. - The entity is conducting prioritization based on the identified Datasets. - The entity is conducting an impact analysis to assess any potential damage of unauthorized access to its identified Datasets and assigning the defined DC levels based on NDMO-SDAIA standards. - The entity is conducting an impact analysis for data classified as low impact. - The entity is implementing the defined Data Handling and Protection Controls based on the classification level for the datasets/artifacts. - The entity is assigning data access rights and privileges across the entity. - The entity is maintaining a register of all identified datasets and artifacts.	All level 2 acceptance evidence including:	DC.3.1
		The Inventory Report of the Identified Datasets and Artifacts.	
		The Prioritized Datasets and Artifacts.	DC.1.2
		Evidences of Utilization of the Data Catalog Tool for the Data Inventory.	
		The Impact Assessment Report.	DC.3.2
		The Assessment Report of Low-Impact Data.	DC.3.3
		The Approved Data Access List of users with the Assigned Privileges.	
Level 4: Managed	The entity is monitoring the effectiveness of the DC processes with pre-defined KPIs.	All level 3 acceptance evidence including:	DC.4.1
		The Monitoring Report of the DC Processes with Pre-defined KPIs.	

Maturity Questions – Data Classification Domain			
DC.MQ.2	Has the entity defined, identified and implemented the required Data Classification (DC) processes?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 5: Pioneer	- The entity is continuously improving the process for DC. - Innovative solutions and tools are explored to proactively scan data and prioritize the classification of data.	All level 4 acceptance evidence including: - The Data Classification Automation Tool.	

Maturity Questions – Data Classification Domain			
DC.MQ.3	Has the entity reviewed all its classified datasets and artifacts to ensure that the classification levels assigned to them are the most appropriate ones as specified by the Data Classification (DC) Policies?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No existing Data Classification (DC) review processes are in place.	- No required documents	
Level 1: Establishing	- Existing DC review activities are on a reactive or ad hoc basis.	- The Current Practices of DC Reviews.	
Level 2: Defined	- The entity defined a review mechanism for all classified datasets and artifacts to be reviewed.	- The DC Review Mechanism.	
Level 3: Activated	- The entity is implementing the defined mechanism for DC reviews for the classified datasets and artifacts across the entity. - The entity is publishing on the Data Catalog the DC levels for the reviewed datasets and artifacts as Metadata.	All level 2 acceptance evidence including: - The Data Classification Review Report.	- DC.3.4
		- An Evidence Document of the Published Classification Levels as Metadata.	- DC.3.5
Level 4: Managed	- The entity is monitoring the DC review mechanism with pre-defined KPIs.	All level 3 acceptance evidence including: - The Monitoring Report of the DC Review Mechanism with Pre-defined KPIs.	

Maturity Questions – Data Classification Domain			
DC.MQ.3	Has the entity reviewed all its classified datasets and artifacts to ensure that the classification levels assigned to them are the most appropriate ones as specified by the Data Classification (DC) Policies?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 5: Pioneer	- The entity is continuously improving its DC review process to ensure optimization.	All level 4 acceptance evidence including: - Data classification review mechanisms review report.	

8.1.14. Personal Data Protection Domain

Maturity Questions – Personal Data Protection Domain			
PDP.MQ.1	Has the entity performed an initial Personal Data Protection (PDP) assessment and developed a plan to address the strategic and operational Privacy requirements?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	- No assessment is done for Personal Data Protection (PDP). - No plan is in place to address Data Privacy requirements.	- No required documents	
Level 1: Establishing	- The entity is aware of the requirements for Data Privacy Management. - The entity conducted an initial PDP Assessment to evaluate the current state of the entity's PDP practices, identified gaps against business and regulatory obligations including the following: 1. Identification of the types of personal data being collected. 2. Location & method of personal data storage. 3. Current processing & uses of the personal data. 4. Privacy challenges to meet compliance with the PDPL rules and executive regulations published by NDMO-SDAIA.	- Evidences of the existing practices of the PDP Domain and Data Privacy.	
		- The Initial PDP Assessment Result.	- PDP.1.1
Level 2: Defined	- The entity developed a plan to address the Strategic and Operational Data-Privacy requirements, including a list of activities, required resources, training courses and a budget.	All level 1 acceptance evidence requirements including: - The Approved PDP implementation plan.	- PDP.1.2
		- The PDP Training plan.	
Level 3: Activated	- The entity is implementing the defined PDP & Data Privacy program in a formalized manner. - This program includes implementing activities which ensure the proactive identification and resolution of potential Privacy issues and risks including training and awareness for all employees to promote a Personal Data Protection-centric culture.	All level 2 acceptance evidence requirements including: - The PDP Plan Implementation Status Report.	
		- Evidence of PDP training activities conducted.	- PDP.2.1

Maturity Questions – Personal Data Protection Domain			
PDP.MQ.1	Has the entity performed an initial Personal Data Protection (PDP) assessment and developed a plan to address the strategic and operational Privacy requirements?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 4: Managed	The entity is monitoring the effectiveness of the PDP plan with pre-defined Key Performance Indicators (KPIs).	All level 3 acceptance evidence requirements including: The Monitoring Report for the PDP Plan with pre-defined KPIs.	
Level 5: Pioneer	The entity periodically reviews its PDP plan to ensure sustained compliance with the applicable regulations, and other environmental requirements or impacts.	All level 4 acceptance evidence requirements including: Review report and continuous improvement of the personal data protection plan.	

Maturity Questions – Personal Data Protection Domain			
PDP.MQ.2	Has the entity defined and implemented Privacy policies and processes for Personal Data including Data breach identification, consent management, Data subject rights, and Privacy risk assessments?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 0: Absence of Capabilities	No practices are in place to identify and address data breach nor privacy violations.	No required documents	
Level 1: Establishing	- The entity identifies data breach or privacy violations on a reactive basis without standardized practices nor policies. - The entity addresses violations when ad hoc Data Privacy interventions occur.	Evidences of the existing initiatives for PDP and Data Privacy.	
Level 2: Defined	- The entity has developed and approved policies and processes for PDP and Data Privacy, including the identification of data breaches, Data Privacy considerations, privacy notice & consent management, and compliance management to comply with the applicable regulations. - Governance has been defined to manage compliance with the PDPL rules and executive regulations published by NDMO-SDAIA in line with the Data Management Organization structure. - The entity has defined a process for Data Subjects' rights management.	The documented data breach notifications process.	
		The documented data breach Management Process.	PDP.3.2
		Entity-Specific PDP Policies.	
		The PDP & Data Privacy Notice and the Consent Management Process.	PDP.4.1
		The Data Subjects' Rights Management Processes.	PDP.4.2

Maturity Questions – Personal Data Protection Domain			
PDP.MQ.2	Has the entity defined and implemented Privacy policies and processes for Personal Data including Data breach identification, consent management, Data subject rights, and Privacy risk assessments?		
Level Name	Level Description	Acceptance Evidence	Related Specification
Level 3: Activated	- The entity is implementing and standardizing the developed and approved practices for PDP including the Consent Management Workflow, notifications to regulatory authority as required and data breach management. - The PDP policies and standardized processes for data subjects rights have been published on the entity's official government website with a feedback mechanism for questions or issues raised by the data subjects. - The entity maintains a register of its compliance records including records of any collection and / or processing of any Personal Data (e.g. Identified Data breach/leakage, etc.). The register is made available to regulators as required.	All level 2 acceptance evidence requirements including: - The Developed & Adopted Consent Management Workflow.	- PDP.4.1
		- Evidences of Notifications Sent to the Regulatory Authority within the Allotted Timeframe.	- PDP.3.1
		- Evidences of data breach management, including identified data breach/leakage.	
		- The Results of the PDP Risk Assessments.	- PDP.4.3
		- Evidences of Published Data Subjects Rights Management Processes and Feedback Received from Data Subjects.	- PDP.4.2
		- The PDP Register.	- PDP.5.1
Level 4: Managed	- The entity monitors the effectiveness of PDP practices and compliance with the PDPL rules and executive regulations, based on the pre-defined Key Performance Indicators (KPIs) in the domain's implementation plan. - The entity is conducting periodic audits on compliance with PDPL rules and executive regulations published by NDMO-SDAIA.	All level 3 acceptance evidence requirements including: - The Monitoring Report for the PDP & Data Privacy Practices with pre-defined KPIs.	
		- The Compliance Monitoring Report & Audit Results.	- PDP.4.4
Level 5: Pioneer	- The entity continuously reviews its PDP practices to ensure sustained compliance with PDPL rules and executive regulations published by NDMO-SDAIA. - Continuous improvement, enabled by automation & change management, is performed in line with the defined regulatory requirements.	All level 4 acceptance evidence requirements including: - The Documented Periodic Reviews & Outcomes for the PDP & Data Privacy Practices.	
		- Evidences of Automation & Change Management for PDP.	



8.2. Appendix II – Acceptance Evidence Checklists

The acceptance evidences outlined in Appendix I are detailed into acceptance criteria in this section. This helps to streamline the assessment journey and ensures coverage of all aspects required for evaluation.

8.2.1. Data Governance Domain

Checklist – Data Governance Domain		
DG.MQ.1	Has the entity established & implemented a Data Management & Personal Data Protection (DM & PDP) Strategy and a DM & PDP Plan with Key Performance Indicators (KPIs) that can be continuously measured to ensure optimization?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents
Level 1: Establishing	- Existing data-related practices.	Attach a report showing current data practices.
Level 2: Defined	- The approved DM & PDP Strategy.	Attach the Data Management and Personal Data Protection (DM & PDP) Strategy which must be approved & includes the following, at a minimum: • Current challenges in DM. • The Strategic requirements including: • Internal requirements emanating from the entity's business strategy. • External requirements emanating from the National Strategy for DM & PDP. • The DM & PDP Vision, Mission, and Strategic Objectives. • Strategic and operational performance indicators with targets extending from 3 to 5 years over the strategy's implementation duration. • The financial budget required to implement the strategy divided according to identified initiatives.
	- The DM guiding principles.	Attach a copy of the DM & PDP program guidelines, which may be a part of the entity's DM & PDP Strategy doc or a separate doc. The guidelines must refer to: • The principles underlying the culture of DM & data processing, to enable and spread a unified DM & PDP concept within the entity itself.
	- Data strategy approval decision letter.	Attach a copy of the entity-specific data strategy approval decision by the entity's Data Management Committee or the entity's authority holder.

Checklist – Data Governance Domain		
DG.MQ.1	Has the entity established & implemented a Data Management & Personal Data Protection (DM & PDP) Strategy and a DM & PDP Plan with Key Performance Indicators (KPIs) that can be continuously measured to ensure optimization?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 3: Activated	- All level 2 acceptance evidence requirements including: - The developed DM & PDP implementation plan.	Attach the implementation plan which must include, at a minimum: • Identified initiatives that covers all the DM domains. • A prioritized list of DM initiatives with descriptions. • A three-year Implementation roadmap to close the gaps identified between the current state and target state.
	- Implementation status report.	Attach a report of the implementation status of DM and PDP plan, including, at a minimum: • Initiatives and projects status: Identifying the status of each initiative or project (started, in progress, completed, or delayed), along with clarification of any delays or challenges. • Progress percentages: Providing the progress percentages of activities and milestones in the plan and roadmap, with clear details on the actual activities that have been completed. • Supporting evidence: Attaching proof of achieved progress/completion, such as reports, photos, documents, or meeting minutes that support the implementation status.
Level 4: Managed	- All level 3 acceptance evidence requirements including: - The monitoring report of the DM & PDP strategy & plan implementation based on the defined KPIs in the strategy & implementation plan.	The entity should attach an updated report approved by the entity's authority holder to monitor the effectiveness of the strategy and implementation plan based on the identified and pre-defined Key Performance Indicators (KPIs) and scorecards. - Each indicator's card should include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.).

Checklist – Data Governance Domain		
DG.MQ.1	Has the entity established & implemented a Data Management & Personal Data Protection (DM & PDP) Strategy and a DM & PDP Plan with Key Performance Indicators (KPIs) that can be continuously measured to ensure optimization?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values.
Level 5: Pioneer	All level 4 acceptance evidence requirements including: - A report demonstrating the entity's monitoring of the latest DM practices and updating of the implementation plan based on these practices and changes in business requirements.	Attach a report showing that the entity identified, implemented and has been monitoring the continuous improvement mechanisms for DM & PDP plan. The report shall include the following: • The updated DM & PDP strategy. • The updated DG practices that include the Data Management Organization, the roles, the processes, & the technologies. • The continuous improvement mechanisms for all DM Domains.
	- A report demonstrating the entity's monitoring of the latest DM practices and updating of the strategy based on these practices and changes in business requirements.	Attach a report showing that the entity identified, implemented and has been monitoring the continuous improvement mechanisms for DM & PDP strategy. The report shall include the following: • The documented periodic DM & PDP reviews & results. • Documented changes to the initial approved plan where applicable.

Checklist – Data Governance Domain		
DG.MQ.2	Has the entity established and implemented Data Management (DM) Policies, Standards and Guidelines across all Data Management (DM) Domains?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents
Level 1: Establishing	- The Data Management & Personal Data Protection (DM & PDP) Policies, Controls and Guidelines Gap Analysis document.	The gap analysis document shall include the following at a minimum: • An analysis of DM & PDP Standards and Guidelines established by the National Data Management Office (NDMO). • Identifying & analyzing all data-related policies & controls published by the Oversight Entities & the regulator(s) of the sector to which the entity belongs. • An analysis of the entity's internal requirements for DM & PDP Controls. • Recommendations and suggestions to close the gaps identified as well as a specific list of policies that the entity will develop in line with the Policies published by NDMO-SDAIA. • A plan to develop DM & PDP policies and controls, clearly presenting the implementation timeline.
Level 2: Defined	All level 1 acceptance evidence requirements including: - The policies, standards, and guidelines developed by the entity for all DM domains.	- The entity should develop policies covering all DM domains, as well as standards and guidelines as needed. The policies should be approved by the Data Management and Governance Committee and every policy's document shall include, the following, at a minimum: • Policy Name. • Release date. • Version number. • Document control (Preparation, review, approval). • Version history. • Terminology. • Goal. • Scope of work. • Guiding Principles • Policy Statement. • Job roles & responsibilities. • Related Policies. • References. • Policy Owner. - The entity should attach the policies approval evidence.

Checklist – Data Governance Domain		
DG.MQ.2	Has the entity established and implemented Data Management (DM) Policies, Standards and Guidelines across all Data Management (DM) Domains?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 3: Activated	All level 2 acceptance evidence requirements including:	Attach the policies implementation status report, showing the percentages of progress in developing the processes and procedures related to policy implementation.
	- Implementation status report.	
	- A document proving the Entity's adoption of the developed policies, standards & guidelines.	Attach a report showing the dissemination and communication of all developed policies to the relevant stakeholders of each policy (e.g., email notifications sent to relevant stakeholders to introduce the approved policies or through the entity's official portal, etc.).
Level 4: Managed	- Approved Compliance Management Framework.	Attach the Compliance Framework, including the following: - The scope of the compliance audit's periodic procedure. - The processes needed to plan and perform the compliance audit procedure. - The processes & tools needed for reporting a compliance audit results. - The processes & plans for remediating & escalating non-compliance cases.
	All level 3 acceptance evidence requirements including:	The entity should attach an updated report, approved by the entity's authority holder, to monitor the performance status of the developed policies and standards based on the identified and pre-defined Key Performance Indicators (KPIs) and scorecards.
	- Monitoring reports on the developed policies and standards, based on the pre-defined KPIs related to these policies and standards, as outlined in the DM strategy and implementation plan.	Each indicator's card should include the following at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value.

Checklist – Data Governance Domain		
DG.MQ.2	Has the entity established and implemented Data Management (DM) Policies, Standards and Guidelines across all Data Management (DM) Domains?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values.
	- The Entity's Compliance Audit Results Report.	Attach a report documenting the results & outputs of each procedure implemented to monitor compliance. The compliance report shall include the following, at a minimum: - Compliance or Non-Compliance with each specification. - An explanation for compliance results with sufficient evidence for each specification. - Recommendations to remediate each instance of non-compliance. - Accountable stakeholder for each recommendation, and the target date to complete the recommendation.
	- Compliance Monitoring Report.	Attach a report(s) to confirm that the entity has established and monitored compliance points by implementing a periodic compliance audit procedure. For the report to be accepted, it must be: - Compliant with the national framework for compliance in data management and governance. - Include compliance audit scores generated by the periodic compliance audits.
Level 5: Pioneer	All level 4 acceptance evidence requirements including: A report demonstrating the entity's innovative mechanisms for enabling compliance monitoring of DM & PDP Policies and Standards.	The entity should attach the continuous improvement report for DM, DG, and PDP policies, based on the results of KPI measurements and relevant updates and developments. The report should include the following, at a minimum: - Conducted Reviews. - Results of each review. - Implemented improvements (with supporting documents). - Innovative mechanisms developed by the entity for enabling compliance monitoring of DM & PDP policies and standards.

Checklist – Data Governance Domain		
DG.MQ.3	Has the entity established and operationalized all roles required for the Data Management Organization as per the NDMO Controls & Specifications?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents
Level 1: Establishing	- The Entity's Data Management Office establishment decision.	Attach the decision to establish a Data Management Office to supervise the implementation of the national strategy for DM, DG & PDP. To accept the attachment, the following requirements must be met: - The decision must be issued by the entity's authority holder. - The Office's responsibilities are documented in line with the "Organizational Manual".
	- The appointment/hiring decisions for the following roles: A. Chief Data Officer (CDO) hiring/ appointment decision letter.	To accept the attachment, the following requirements must be met: - The decision must be issued by the entity's authority holder. - The CDO's responsibilities are clarified in an approved job description. - The responsibilities are in line with the "Organizational Manual".
	- The appointment/hiring decisions for the following roles: B. Data Management Officer / Data Governance Officer Hiring / Appointment Decision.	To accept the attachment, the following requirements must be met: - The decision must be issued by the entity's authority holder. - The Data Management Officer / Data Governance Officer's responsibilities are clarified in an approved job description. - The responsibilities are in line with the "Organizational Manual".
Level 2: Defined	All level 1 acceptance evidence requirements including: - Data Management & Governance Committee formation decision.	To accept the attachment, the following requirements must be met: - The decision must be issued by the entity's authority holder. - The Committee's Charter including: - Roles and Responsibilities. - Rules of work for the committee. The decision letter must include a statement indicating that the committee's tasks involve providing guidance and overseeing the DM Strategy at the organizational level.
	- The Hiring / Appointment decisions of the following roles: A. Compliance Officer Hiring / Appointment Decision.	To accept the attachment, the following requirements must be met: - The decision must be issued by the entity's authority holder. - The Compliance Officer's responsibilities are clarified in an approved job description. - The responsibilities are in line with the "Organizational Manual".

Checklist – Data Governance Domain		
DG.MQ.3	Has the entity established and operationalized all roles required for the Data Management Organization as per the NDMO Controls & Specifications?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Hiring / Appointment decisions of the following roles: B. Business Data Executive Hiring / Appointment Decision.	To accept the attachment, the following requirements must be met: • The decision must be issued by the entity's authority holder. • The Business Data Executive's responsibilities are clarified in an approved job description. • The responsibilities are in line with the "Organizational Manual".
	- The Hiring / Appointment decisions of the following roles: C. Legal Advisor Hiring / Appointment Decision.	To accept the attachment, the following requirements must be met: • The decision must be issued by the entity's authority holder. • The Legal Advisor's responsibilities are clarified in an approved job description. • The responsibilities are in line with the "Organizational Manual".
Level 3: Activated	All level 2 acceptance evidence requirements including: - The Hiring / Appointment decisions of the following roles: A. Business Data Steward(s) Hiring / Appointment Decision.	To accept the attachment, the following requirements must be met: • The decision must be issued by the entity's authority holder. • The Business Data Steward's responsibilities are clarified in an approved job description. • The responsibilities are in line with the "Organizational Manual".
	- The Hiring / Appointment decisions of the following roles: B. List of the IT Data Stewards.	To accept the attachment, the following requirements must be met: • The decision must be issued by the entity's authority holder. • The IT Data Steward's responsibilities are clarified in an approved job description. • The responsibilities are in line with the Organizational Manual.
	- The Hiring / Appointment decisions of the following roles: C. Personal Data Protection (PDP) Officer Hiring / Appointment Decision.	To accept the attachment, the following requirements must be met: • The decision must be issued by the entity's authority holder. • The PDP Officer's responsibilities are clarified in an approved job description. • The responsibilities are in line with the Organizational Manual.

Checklist – Data Governance Domain		
DG.MQ.3	Has the entity established and operationalized all roles required for the Data Management Organization as per the NDMO Controls & Specifications?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Hiring / Appointment decisions of the following roles: D. Open Data and Information Access Officer Hiring / Appointment Decision.	To accept the attachment, the following requirements must be met: - The decision must be issued by the entity's authority holder. - The ODIAO's responsibilities are clarified in an approved job description. - The responsibilities are in line with the Organizational Manual.
	The documented & approved Data Management Organization structure.	Attach the documented & approved Data Management Organization structure, including the following, at a minimum: - Roles & responsibilities. - Approved job descriptions for each role. - Authorization: Reviews, approvals and decision making.
	The documented Data Stewardship / Ownership structure.	Attach the documented & approved Data Stewardship / Data Ownership structure, including the following, at a minimum: - Identified Data Domains. - Business Data Executives for each Data Domain. - Business Data Steward for each Data Domain. - IT Data Steward for each Data Domain. - Roles & responsibilities.
Level 4: Managed	All level 3 acceptance evidence requirements including The monitoring reports for the entity's Data Management Organization roles based on the pre-defined KPIs in the strategy and implementation plan.	The entity should attach an updated report approved by the entity's authority holder to measure the entity's performance in monitoring job roles based on the identified and pre-defined Key Performance Indicators (KPIs) and scorecards. Each indicator's card should include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually).

Checklist – Data Governance Domain		
DG.MQ.3	Has the entity established and operationalized all roles required for the Data Management Organization as per the NDMO Controls & Specifications?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values.
Level 5: Pioneer	All level 4 acceptance evidence requirements including: Continuous improvement report for the roles and responsibilities of Data Management Organization within the entity.	The entity must attach the continuous improvement report for the roles and responsibilities of DM Organization within the entity. The report should include the following, at a minimum: - Conducted Reviews. - Results of each review. - Implemented improvements (with supporting documents).

Checklist – Data Governance Domain		
DG.MQ.4	Has the entity established and implemented practices for Change Management including awareness, communication, change control, and capability development?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents
Level 1: Establishing	Evidences of communication on DM-related practices.	Attach evidences showing that the entity has communications regarding Data Management practices, such as: - E-mails. - Correspondences.

Checklist – Data Governance Domain		
DG.MQ.4	Has the entity established and implemented practices for Change Management including awareness, communication, change control, and capability development?	
Levels	Acceptance Evidence	Acceptance Criteria
	Evidences of training and awareness sessions conducted.	Attach a report on the training courses & awareness programs implemented by the entity, including the following, at a minimum: - Names of the implemented training courses related to DM, DG & PDP. - Awareness programs implemented in the different Domains under DM, DG & PDP. - A certificate of attendance sample for training the entity's employees in Domains related to DM, DG & PDP.
Level 2: Defined	All level 1 acceptance evidence requirements including: The Change Management Plan.	The Change Management Plan covering all DM Domains including, at a minimum: - The DM & PDP Training Plan for all DM Domains. - The DM Communication plan. - The Stakeholders engagement plan. - The Change Control plan for data system changes.
Level 3: Activated	All level 2 acceptance evidence requirements including: The Change Management Implementation Status Report showing the DM & PDP Training & Awareness Activities.	Attach a report on the implementation status of the change management plan, and the report must include, at a minimum: - The DM & PDP Training implementation status for all DM Domains showing: - Evidences of training conducted for the entity's employees, covering all DM Domains. - A list of activities carried out by the entity to raise awareness regarding the national regulations, laws, policies & controls, standards and their applicability (such as: e-mails, publications, lectures, workshops, etc.). - A list of activities carried out by the entity to raise awareness regarding the national DM, DG & PDP strategy and programs and their applicability on the entity (such as: e-mails, publications, lectures, workshops, etc.). - A list of activities carried out by the entity to raise awareness regarding the data management domains as per the National Data Management and Personal Data Protection Framework, addressed to the related Data Management and Personal Data Protection roles.
	The Change Management Implementation Status Report showing the DM Communication activities.	Attach a report on the implementation status of the change management plan, and the report must include evidences confirming the entity's continuous communication regarding the following: - The DM, DG & PDP Program, activities and main decisions. - The storage of DM & DG documents & artifacts. - The measurement of DM & DG performance indicators. - The updates on DM & DG policies & processes. - The updates on compliance reports, implementation plans, and the regulatory (legislative) environment related to DM & DG.

Checklist – Data Governance Domain		
DG.MQ.4	Has the entity established and implemented practices for Change Management including awareness, communication, change control, and capability development?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Stakeholders Engagement and Socialization Plan implementation status report.	Attach a report showing that the entity is engaging the identified stakeholders to develop and improve on the capabilities of the DM & PDP program.
	- The Data Governance Approvals Register.	The register should include, at a minimum: - CDO's DG Decisions with their rationalized constituents. - DM & DG Committee Decisions.
	- The Data Management Issue Tracking Register.	The register should include, at a minimum: - A sample of DM & DG issues reported by business & technical users. - Evidence of resolution of the reported issues.
	- Evidences that the Entity has DM & DG document & artifact Version Control practices.	Attach a sample of a register / record or a document created by the entity, and it must include the following at a minimum: - The Domain name of the registry. - The Registry's Issuance Date. - The Registry's Updating Dates. - The Registry Versions Control. - The Updates made to the Registry or document.
Level 4: Managed	All level 3 acceptance evidence requirements including: The monitoring report of the change management practices with pre-defined KPIs in the Change Management Plan.	A report on monitoring the Change Management activities & practices should be attached based on pre-defined KPIs, which include, at a minimum, the following indicators: - The Indicator of the periodic meetings of the internal DM & DG & PDP committee. - The Indicator of the completed training & awareness sessions. - The Indicator of the attendance rates in the completed training & awareness sessions. - The duration Indicator of the DM & PDP issue resolutions. - The quantity Indicator of the number of resolved & closed change requests. Each indicator's card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation.

Checklist – Data Governance Domain		
DG.MQ.4	Has the entity established and implemented practices for Change Management including awareness, communication, change control, and capability development?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values.
Level 5: Pioneer	All level 4 acceptance evidence requirements including: Continuous improvement report of the change management, highlighting the innovative mechanisms contributing to change management in areas related to data management.	The entity should attach the continuous improvement report for change management practices, based on the results of KPI measurements and the innovative mechanisms and methods developed by the entity to enhance the effectiveness of change management. The report should include the following, at a minimum: - Conducted Reviews. - Results of each review. - Implemented improvements (with supporting documents). - Innovative mechanisms and methods related to change management.

8.2.2. Metadata and Data catalog Domain

Checklist – Metadata and Data Catalog Domain		
MCM.MQ.1	Has the entity developed and implemented a plan to integrate and manage Metadata across the entity?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	No required documents.
Level 1: Establishing	- The Recorded or Documented Metadata Report.	The entity must attach a report on the Metadata recorded or documented as part of any project's implementation, or in standalone applications.
Level 2: Defined	- The Approved Metadata and Data Catalog Plan.	The entity must attach a recent plan approved by the entity's authority holder for MCM tool / solution implementation plan including the following, at a minimum: - A roadmap that includes the projects and milestones of the technological tool / solution implementation for the Data Catalog. The activities shall incorporate what is needed to achieve this Domain's specifications, at a minimum. - The assignment of the required resources & budget allocation to manage the implementation of the Data Catalog Automation tool.
	- The Approved Metadata Structure.	The entity must attach an updated and approved report illustrating the approved Metadata architecture and Metadata framework. The report must include the following, at a minimum: - The Business Metadata fields to be filled in the Data Catalog. - The additional fields based on the entity's requirements and any other regulatory requirements must be documented in the Data Catalog.
Level 3: Activated	- The Metadata and Data Catalog Plan Implementation Status Report.	The entity must attach an updated and approved report clarifying the MCM Plan implementation status and roadmap which include the following, at a minimum: Initiatives and projects status: identifying the status of each initiative or project (started, in progress, completed, or delayed), along with clarification of any delays or challenges. Progress percentages: Providing the progress percentages of activities and milestones in the plan and roadmap, with clear details on the actual activities that have been completed. Supporting evidence: Attaching proof of achieved progress/completion, such as reports, photos, documents, or meeting minutes that support the implementation status.
	- The Approved Metadata Structure Implementation Report	- The entity must attach an updated and approved report clarifying the Metadata structure implementation status.

Checklist – Metadata and Data Catalog Domain		
MCM.MQ.1	Has the entity developed and implemented a plan to integrate and manage Metadata across the entity?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 4: Managed	- The Monitoring Report with Pre-defined Key Performance Indicators (KPIs) for the Metadata and Data Catalog Plan and Activities.	- The entity must attach an updated monitoring report on the MCM Plan and activities, prepared based on pre-defined KPIs (Indicator Cards), approved by the entity's authority holder. - e.g.: The indicators may include measuring the achievement percentages of the plan implementation requirements. - Each indicator's card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values.
Level 5: Pioneer	- The Continuous Improvement Report on the Metadata and Data Catalog Plan.	- The entity must attach the updated continuous improvement report, approved by the entity's authority holder demonstrating the continuous improvement of the metadata integration and management plan across the entity, and based on the results of KPI measurements and relevant updates and developments in the domain. The report should include the following, at a minimum: • Conducted Reviews. • Results of each review. • Implemented improvements (with supporting documents).

Checklist – Metadata and Data Catalog Domain		
MCM.MQ.1	Has the entity developed and implemented a plan to integrate and manage Metadata across the entity?	
Levels	Acceptance Evidence	Acceptance Criteria

Checklist – Metadata and Data Catalog Domain		
MCM.MQ.2	Has the entity implemented a Metadata Management and Data Catalog tool / solution?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- Evidences of Current Existing Metadata.	- The entity must attach a report proving the existence of the identified Metadata within standalone applications or for a specific project.
Level 2: Defined	- The Selected Data Catalog Tool.	- The entity must attach an approved report clarifying the technology / tool chosen for the Data Catalog (The information includes: The Vendor, version, and specifications).
	- The Approved and Prioritized Data Sources Report.	- The entity must attach an approved report that includes the following, at a minimum: - The Data Catalog Sources where each Source has an approved priority. - The definitions of the entity's business Metadata and the technical Metadata.

Checklist – Metadata and Data Catalog Domain		
MCM.MQ.2	Has the entity implemented a Metadata Management and Data Catalog tool / solution?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Developed and Approved Target Metadata Architecture.	- The entity must attach an approved report clarifying the developed and approved target Metadata architecture including (but not limited to), the following: • Metadata Sources: the entity's Data Sources that are sources of Metadata used in the Data Catalog. • Metadata Repository: the Data Catalog as the entity's central Metadata Repository. • Metadata Flows: A definition of Metadata Flow between the Metadata Sources and the Metadata Repository. • Metadata Model: A Metadata Model used by the entity's Data Catalog.
	- The Data Catalog Tool Implementation Requirements Report.	- The entity must attach an approved report clarifying the Data Catalog tool implementation requirements, including the following, at a minimum: • The procurement approval for a tool to automate the Data Catalog. • The approved plan to implement the Data Catalog automation tool.
	- The Approved and Developed Data Catalog Training Plan.	The entity must attach the recent and developed training and awareness plan approved by the entity's authority holder regarding the Data Catalog usages, including the following, at a minimum: • The training and awareness plan's approval and validity / expiry dates. • The training and awareness programs plan implementation dates. • The scope of the training and awareness. • The objectives of the training and awareness. • The training shall include the following: • An overview of the Data Catalog concept and benefits. • Introductory and advanced lessons on the Automated Data Catalog Tool and its functionalities.

Checklist – Metadata and Data Catalog Domain		
MCM.MQ.2	Has the entity implemented a Metadata Management and Data Catalog tool / solution?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Practical (Hands on) exercises based on use cases on the automated Data Catalog tool. - The training and awareness target audiences. - The topics of the training programs and awareness campaigns. - The methods and channels through which the Training plan will be conducted. - Identifying the MCM Domain Awareness campaign channels, which include: - E mails or mobile phone messages. - Publications. - Lectures or workshops.
Level 3: Activated	- Evidence of the Implemented Data Catalog Tool.	- The entity must attach a report on the Data Catalog tool proving the tool is implemented in the entity.
	- Data Access Approval Process Documentation (Authorization to Connect the Data Catalog with the Data Sources).	- The entity must attach an approved report about the documentation of the approval process for granting authorization access to the entity's data by connecting the Data Catalog tool to the entity's Data Sources.
	- Metadata Access Approval Process Documentation.	- The entity must attach an approved report about the documentation of the approval process for granting scope-based authorization access to the Metadata, including the following, at a minimum: - The name of the system / tool and version number. - A description of the access granting and approval process. - A sample of role-based access groups.
	- Evidences of Data Catalog Adoption and Usage Including Metadata Populated on the Tool.	- The entity must attach a report proving the adoption and usage of the Data Catalog, with evidence for populating Metadata in the tool, including the following, at a minimum: - The identified Data Catalog power users – The entity's Data Catalog advanced users who can act as coaches for other users. - The Communication plan between the current Data Catalog power users and the other Data Catalog users to activate the Data Catalog usage. The plan must include (but not limited to) the following: - A description of the communication procedure actions & processes. - The required frequency of the communication processes. - The target audience.

Checklist – Metadata and Data Catalog Domain		
MCM.MQ.2	Has the entity implemented a Metadata Management and Data Catalog tool / solution?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Regular Audits Report on the Data Catalog Usage.	- The entity must attach the periodic audits report on the Data Catalog usage, including the following, at a minimum: • An audit sample of information about the Data Catalog users. • An audit sample of processes / operations performed by the users. • An audit sample of the Data Catalog activity memory and separately maintained logs of the tracking functionality / audit-trail.
	- Evidence of Training Conducted for the Identified Data Catalog Users.	- The entity must attach a report proving the implementation of the training & awareness programs conducted for the identified Data Catalog users based on the plan. The report must include the following, at a minimum: • The list of conducted training programs and awareness campaigns (Including the topics of the programs, the dates when they were conducted, and the names of the training attendants). • Samples of the activities performed by the entity to raise awareness about the MCM Domain, including: • E mails or mobile phone messages. • Publications. • Lectures or workshops. • A sample attendance certificate of training the entity's employees.
	- Tool Versioning Report.	- The entity must attach a Tool Versioning report including the following, at a minimum: • The name of the developer of the current tool used by the entity. • The number of the current version used by the entity. • The current version's release date within the entity. • The number and date of the latest tool version published by the developer. • The Methodology of the Version Management Strategy (Releasing versions of technological solutions and tools for the Data Catalog) followed in cases where there are issues that prevent upgrading the current version to the latest version.
Level 4: Managed	- The Monitoring Report with Pre-defined KPIs for the Adoption and Usage of the Metadata & Data Catalog Solution / Tool.	- The entity must attach an updated report approved by the entity's authority holder on measuring the effectiveness of the Metadata solution implementation and the Data Catalog usage based on pre-defined and identified KPIs and indicator cards, which cover: • The number of registered Data Catalog users. • The number of active Data Catalog users.

Checklist – Metadata and Data Catalog Domain		
MCM.MQ.2	Has the entity implemented a Metadata Management and Data Catalog tool / solution?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The number of logins to the Data Catalog. - The number of performed Metadata queries. - The number of annotations (tags, comments) added to the Data assets. - The number of ratings added to data assets. - The number of trust certificates assigned to the Metadata. - Each indicator's card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values.
	The Approved List of Pre-defined KPIs for the Quality of the Metadata which is Populated on the Data Catalog Tool.	- The entity must attach a list of approved KPIs (Indicator Cards) pre-defined to monitor the Metadata Quality, including the following, at a minimum: - Completeness. - Accuracy. - Consistency.

Checklist – Metadata and Data Catalog Domain		
MCM.MQ.2	Has the entity implemented a Metadata Management and Data Catalog tool / solution?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Each indicator's card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values.
Level 5: Pioneer	- The Continuous Improvement Report on the Metadata and Data Catalog Tool's quality.	- The entity must attach an updated & approved report presenting continuous improvement on the quality of metadata & Data Catalog tool based on the results of KPI measurements and relevant updates and developments in the domain, including the following, at a minimum: • The documents of periodic reviews & documented results. • Continuous improvement mechanisms and implemented enhancements (with supporting documents). • Resources assigned for implementing the continuous improvement plan.
	- The Metadata Management Automation Report.	- The entity must attach an updated and approved report proving the full automation of end to end Metadata Management using a fully implemented Data Catalog tool, e.g.: Automating Metadata collection and exchange (Evidence such as reports, screenshots, etc...).

Checklist – Metadata and Data Catalog Domain		
MCM.MQ.3	Has the entity defined and implemented formal processes for effective Metadata Management, such as: prioritization, population, access management, and quality issue management, etc., supported & fostered by collaboration across the entity?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- Evidence of the Existing Processes Used to Manage Metadata.	- The entity must attach a document of the current Processes followed for Metadata Management (Evidence such as reports, screenshots, etc...).
Level 2: Defined	- Metadata Identification Process Report.	- The entity must attach a report showing the entity's process for identifying and defining its business and technical metadata that will be included in the Data Catalog.
	- Metadata Prioritization Process Report.	- The entity must attach a report showing the entity's process for prioritizing the identified metadata.
	- Metadata Population Process Report.	- The entity must attach a report showing the process for registering and populating the Metadata within the Data Catalog so that the process is implemented as a workflow plan within the automated Data Catalog tool.
	- Metadata Update Process Report.	- The entity must attach a report showing the process for updating metadata in its Data Catalog so that the process is implemented as a workflow plan within the automated Data Catalog tool.
	- Metadata Quality Process Report.	- The entity must attach a report showing the process for identifying and resolving quality issues with the Metadata. This Metadata Management process should include a mechanism for reporting identified data quality issues and development of remediation actions within defined SLAs so that the process is implemented as a workflow plan within the automated Data Catalog tool.
	- Metadata Annotation Process Report.	- The entity must attach a report showing the process for regularly reviewing the metadata annotations (tags, comments) made by users to the Metadata within the Data Catalog so that the process is implemented as a workflow plan within the automated Data Catalog tool.
	- Metadata Certification Process Report.	- The entity must attach a report showing the process for regularly reviewing the trust certificates assigned by users to the Metadata within the Data Catalog so that the process is implemented as a workflow within the automated Data Catalog tool.
Level 3: Activated	- Evidence of the Implementation and Adoption of the Approved Processes as Workflows in the Entity's Data Catalog.	- The entity must attach an approved report proving the implementation and adoption of the approved processes, including each process's workflow chart. The processes must include the following, at a minimum: • Metadata Identification Process.

Checklist – Metadata and Data Catalog Domain		
MCM.MQ.3	Has the entity defined and implemented formal processes for effective Metadata Management, such as: prioritization, population, access management, and quality issue management, etc., supported & fostered by collaboration across the entity?	
Levels	Acceptance Evidence	Acceptance Criteria
		• Metadata Prioritization Process. • Metadata Population Process. • Metadata Updating process. • Metadata Quality Process. • Metadata Annotation Process. • Metadata Certification Process. - The entity must attach a recent, approved report demonstrating the business metadata registered in the entity's metadata repository. - The entity must attach a recent, approved report demonstrating the technical metadata registered in the entity's metadata repository.
	- The Logs or the List of Notifications on the Metadata Changes.	The entity must attach a report that includes the logs, or a list of alerts caused by Metadata changes.
	- Evidences of Communications to the Data Catalog Users of any Metadata Update.	The entity must attach the implementation report of contacting the Data Catalog users (e.g.: emails) when any Metadata is updated.
	- The Metadata Stewardship Coverage Model.	The entity must attach a report clarifying the Metadata Stewardship Coverage Model.
Level 4: Managed	- The Metadata Processes Monitoring Report with Pre-Defined KPIs.	The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of metadata processes implementation based on pre-defined and indicated KPIs and Indicator Cards, - Each indicator's card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually).

Checklist – Metadata and Data Catalog Domain		
MCM.MQ.3	Has the entity defined and implemented formal processes for effective Metadata Management, such as: prioritization, population, access management, and quality issue management, etc., supported & fostered by collaboration across the entity?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values.
	- The Metadata Quality Monitoring Report with Pre-Defined KPIs.	- The entity must attach an updated report approved by the entity's authority holder on monitoring the metadata quality based on pre-defined KPIs (Indicator Cards) including the following, at a minimum: - Completeness. (completeness level of business and data dictionaries) - Accuracy. (extent of alignment between definitions and descriptions with business context) - Consistency. (extent of consistency of metadata definitions across all departments within the entity) - Each indicator's card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target).

Checklist – Metadata and Data Catalog Domain		
MCM.MQ.3	Has the entity defined and implemented formal processes for effective Metadata Management, such as: prioritization, population, access management, and quality issue management, etc., supported & fostered by collaboration across the entity?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values.
Level 5: Pioneer	- The Continuous Improvement Report on the Metadata Management Practices.	- The entity must attach an updated & approved report presenting continuous improvement of metadata management practices based on the results of the KPI measurements and relevant updates and developments in the domain including the following, at a minimum: - The documents of the periodic reviews & documented results of the Metadata Management Practices. - The continuous improvement mechanisms of the metadata management practices and implemented improvements (with supporting documents).

8.2.3.Data Quality Domain

Checklist – Data Quality Domain		
DQ.MQ.1	Has the entity developed and implemented a Data Quality (DQ) plan focused on improving the quality of the entity's Data?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents
Level 1: Establishing	- Evidence of the Existing Data Quality (DQ) Related Activities.	The entity must attach a report on the activities that are practiced in the DQ Domain. For each activity, the report must contain the following, at a minimum: - Copies / screenshots of e-mail correspondences which support practicing the activity. - Copies / screenshots of documents which support practicing the activity. - Screenshots of the systems which support practicing the activity.
Level 2: Defined	- The Defined and Approved DQ Implementation Plan.	The entity must attach a recent and defined DQ management plan approved by the entity's authority holder to implement and manage the activities which aim at improving the entity's data. This plan must contain the following, at a minimum: - A roadmap that includes the activities and milestones of implementing the DQ Management practices in the entity. The activities shall incorporate what is needed to achieve this Domain's specifications, at a minimum. - The assignment of the required resources & budget allocation to manage the implementation of the DQ Management Plan.
Level 3: Activated	- A Report on the DQ Plan Implementation Status.	The entity must attach an updated & approved report on the DQ plan implementation status and roadmap containing the following, at a minimum: Initiatives and projects status: Identifying the status of each initiative or project (started, in progress, completed, or delayed), along with clarification of any delays or challenges. Progress percentages: Providing the progress percentages of activities and milestones in the plan and roadmap, with clear details on the actual activities that have been completed. Supporting evidence: Attaching proof of achieved progress/completion, such as reports, photos, documents, or meeting minutes that support the implementation status.
	- A Report on the Defined DQ Roles & Responsibilities.	The entity must attach an updated & approved report presenting the implementation status of the DQ Domain's defined roles and responsibilities containing the following, at a minimum: - The DQ Roles of the Data Stewards. - The Responsibilities of the Data Stewards in the DQ Domain operations. - A list of employees assigned to carry out the defined roles for DQ.

Checklist – Data Quality Domain		
DQ.MQ.1	Has the entity developed and implemented a Data Quality (DQ) plan focused on improving the quality of the entity's Data?	
Levels	Acceptance Evidence	Acceptance Criteria
	- A Report on the Assigned Resources for the DQ Plan.	The entity must attach an updated & approved report presenting the current status of the resources allocated for the implementation of the DQ activities containing the following, at a minimum: • The people, processes and tools needed to implement the DQ activities.
Level 4: Managed	- The Monitoring Report of the DQ Plan and Activities with Pre-defined Key Performance Indicators (KPIs).	- The entity must attach an updated report, approved by the entity's authority holder on measuring the effectiveness of DQ implementation plan based on pre-defined and identified KPIs and indicator cards. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The Continuous Improvement Report of the Data Quality Plan & Activities.	- The entity must attach an updated & approved report presenting continuous improvement based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: • Reviews conducted. • Results of each review.

Checklist – Data Quality Domain		
DQ.MQ.1	Has the entity developed and implemented a Data Quality (DQ) plan focused on improving the quality of the entity's Data?	
Levels	Acceptance Evidence	Acceptance Criteria
		Improvements implemented (with supporting documents).

Checklist – Data Quality Domain		
DQ.MQ.2	Has the entity established / developed and implemented practices to manage and improve the quality of the entity's data?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- The Existing DQ Domain Initiatives.	- The entity must attach a report on the current DQ Domain initiatives.
	- The Existing Processes for Detecting DQ Issues.	- The entity must attach a report on the current DQ issue detection processes.
	- The Existing Processes Used for Data Corrections or Data Validations.	- The entity must attach a report on the current processes used for data corrections or data validations.
Level 2: Defined	- The Prioritized List of Data Elements.	- The entity must attach a report listing the data elements ranked / prioritized based on business requirements. The first priority data must include the entity's Master Data, at a minimum.
	- The Defined DQ Dimensions for the Entity's Datasets.	- The entity must attach a report clarifying the defined DQ Dimensions for the entity's Datasets including the following, at a minimum: • Completeness (The degree of how complete data records are). • Uniqueness (The degree of how unique data records are without duplicates). • Timeliness (The degree to which data is up to date and available when it is needed). • Validity (The degree of records' conformance to the established formats, types and ranges). • Accuracy (The degree to which data values align to real values). • Consistency (The degree to which data is consistent across the entity's business and across different sources).
	- The Data Quality Rules Report.	- The entity must attach a report clarifying the list of defined DQ Rules that are aligned with the DQ Dimensions including the following, at a minimum: • The DQ rule owner. • The business description of the requirement to be validated by the rule.

Checklist – Data Quality Domain		
DQ.MQ.2	Has the entity established / developed and implemented practices to manage and improve the quality of the entity's data?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Regarding the particular data whose quality is being measured: The assignment of Rules to each of the DQ Dimensions including the following, at a minimum: - Completeness. - Uniqueness. - Timeliness. - Validity. - Accuracy. - Consistency. - The list of Data Attributes validated by the defined rules. - The metrics that are calculated when validating each DQ rule. - The escalation threshold that triggers a DQ alert for the rule.
	The Developed & Approved Processes for DQ Issue Management & Remediation.	- The entity must attach a report clarifying the Developed & Approved Processes for DQ Issue Management & Remediation followed for DQ issue management & remediation / resolution including, at a minimum, the following: - Developing a remediation plan. The remediation plan must include the following, at a minimum: - A "Root Cause" analysis to determine the causes of the identified DQ issue. - An Impact analysis to assess the negative consequences and determine an issue level (whether it is local / limited, or at the entity level). - The definition & identification of the DQ Targets set for each of the issues & challenges, related to each DQ Dimension, depending on the context of the issue / challenge within the entity. - The definition & identification of the options for resolving the issue's "Root Cause", including a feasibility analysis. - The specifications of the Data Cleansing process to be performed if the solution does not correct the "Root Cause" of the DQ issue. - The decision & the logical rationale for selecting the specific option (chosen) to solve the issue. - The implementation status of the issue's most suitable resolution choice (including any change).

Checklist – Data Quality Domain		
DQ.MQ.2	Has the entity established / developed and implemented practices to manage and improve the quality of the entity's data?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The review of the implemented resolution and a verification that the issue is resolved. - Establishing & developing a roadmap and milestones for the resolution of the noticed & identified DQ issues. - Allocating the necessary resources to implement the DQ issue identification plan.
Level 3: Activated	- The Planned & Conducted Initial & Periodic Data Quality Assessment Report.	- The entity must attach a report clarifying the initial & periodic DQ assessment, which was planned for and conducted (already). The assessment must include the following, at a minimum: - Collecting business requirements for the Quality of Data in the scope. - Establishing & defining DQ Rules based on the collected business requirements specifically. - Performing a check by Data Profiling based on the pre-defined DQ Rules. - Reporting the discovered and identified DQ comments & issues to the concerned / relevant department in the entity. - Developing plans (with key milestones) for resolving the discovered & identified DQ issues.
	- The Resolution Status Report of the Identified DQ Issues.	- The entity must attach a report presenting the resolution status of the identified DQ issues, including: - The implementation status of the issue's most suitable resolution choice. - The review of the implemented resolution and a verification that the issue is resolved.
	- Evidences of DQ Tools Used for Automating DQ Issue Management Workflows.	- The entity must attach a report showing the activation of DQ tools used to implement DQ issue management and presenting the following tools capabilities, at a minimum: - Data Profiling Statistical data analysis on the following levels: data attributes, tables, cross Domain and different systems. - DQ Rules Management DQ rules establishment, development and execution. - DQ Issues Management Automation of workflows for reporting and resolving DQ issues.
	- The Defined & Implemented DQ Service Level Agreements (SLAs).	- The entity must attach the defined DQ SLAs including the following, at a minimum: - A timeline and a deadline for the development of a remediation plan for the identified DQ issue. - A timeline and a deadline for the implementation and the review of the DQ changes. - The escalation procedures to be taken when the SLA is not met.

Checklist – Data Quality Domain		
DQ.MQ.2	Has the entity established / developed and implemented practices to manage and improve the quality of the entity's data?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The List of DQ System Enforcements Adopted by the Entity.	- The entity must attach a report clarifying the list of DQ System Enforcements adopted by the entity (e.g., The Standard Implementation Mechanism & the Standard Implementation Result).
Level 4: Managed	- The Monitoring Report of the DQ Management Practices with Pre-defined KPIs.	- The entity must attach an updated report, approved by the entity's authority holder on measuring the effectiveness of implementing DQ improvement practices based on pre-defined and identified KPIs and indicator cards. These KPIs must include the following, at a minimum: • The number of resolved data quality issues compared to the total number of reported data quality issues. • The number of resolved data quality issues that exceeded their scheduled resolution deadlines. • The total time spent to develop a remediation plan for a discovered data quality issue. • The total time spent to resolve a data quality issue (implementing a "root cause" solution). - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values.

Checklist – Data Quality Domain		
DQ.MQ.2	Has the entity established / developed and implemented practices to manage and improve the quality of the entity's data?	
Levels	Acceptance Evidence	Acceptance Criteria
		Supporting documents for the data used to calculate the indicator values
	- The Monitoring Report of the DQ Threshold Values.	- The entity must attach an approved report on monitoring and updating the threshold Values for each DQ Rule.
	- The Monitoring Report of the DQ Issue Resolution Process.	- The entity must attach an updated & approved monitoring report on the DQ issue resolution process including the following, at a minimum: - The number of resolved DQ issues vs the number of reported DQ issues. - The number of DQ issues resolved after the specified deadlines. - The total time of remediation plan development for a discovered DQ issue. - The total time of resolving a DQ issue (A "Root Cause" resolution implementation).
Level 5: Pioneer	- The Continuous Improvement Report on the Tools Used for DQ.	- The entity must attach an updated & approved report showing that the entity is periodically monitoring & regularly optimizing the tools used for DQ based on the results of the KPI measurements and relevant updates and developments in the domain. The report must contain the following, at a minimum: - Reviews conducted. - Results of each review. - Improvements implemented (with supporting documents).
	- The Continuous Improvement Report on the DQ Management Practices.	- The entity must attach an updated & approved report showing that the entity identified, implemented, and is regularly monitoring the continuous improvement mechanisms of the DQ Domain practices, based on the results of the KPI measurements and relevant updates and developments in the domain. The report must contain the following, at a minimum: - Reviews conducted. - Results of each review. - Improvements implemented (with supporting documents).

Checklist – Data Quality Domain		
DQ.MQ.2	Has the entity established / developed and implemented practices to manage and improve the quality of the entity's data?	
Levels	Acceptance Evidence	Acceptance Criteria
		Results of measuring the impact of data quality management practices on improving the entity's data quality across all its systems based on its targets (with supporting documents).
	- The Implemented / Adopted DQ Industry Standards.	- The entity must provide evidence of the adopted DQ Management Standards (e.g., ISO 8000).

Checklist – Data Quality Domain		
DQ.MQ.3	Has the entity established and implemented practices to monitor and report the entity's Data Quality (DQ) status?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- The Existing DQ Monitoring Practices.	- The entity must attach an updated & approved report clarifying the entity's current DQ monitoring practices.
	- Evidence of the Entity's Current DQ Status.	- The entity must attach an updated & approved report showing the current DQ situation.
Level 2: Defined	- The Defined and Formalized DQ Monitoring Plan.	- The entity must attach the defined DQ monitoring plan showing activities required to monitor and document the data quality status on a regular with the assigned resources for implementation.
	- The Defined DQ Checkpoints Report.	- The entity must attach a report clarifying specific Checkpoints defined for DQ Monitoring.
Level 3: Activated	- DQ Scorecards or Dashboards.	- The entity must attach a report illustrating DQ scorecards or DQ dashboards. This should include the following, at a minimum: - Execution of the defined DQ rules which according to defined triggering conditions (time schedule, event). - Reporting of the noticed and identified DQ issues to Data Stewards & Owners, (At a minimum: A Business Data Steward & a Business Data Executive).

Checklist – Data Quality Domain		
DQ.MQ.3	Has the entity established and implemented practices to monitor and report the entity's Data Quality (DQ) status?	
Levels	Acceptance Evidence	Acceptance Criteria
	- A Report on the Data Quality Metadata Logged on the Data Catalog Tool.	- The entity must attach a report presenting the DQ Metadata registered in the Data Catalog Tool as per the process identified in the MCM Domain (Data Catalog & Metadata Management / Management of the Catalog & Metadata). The DQ Metadata must include the following, at a minimum: - The existing DQ Rules. - The DQ Monitoring process results.
	- Evidence of a Data Quality Support Process Implemented as a Workflow.	- The entity must attach a report illustrating DQ Support implemented as a workflow process to solve the issues discovered during the DQ reviews. The report must include the following, at a minimum: - A clear process that enables data users to report DQ issues to Business Data Stewards. - A workflow plan in the automated Data Catalog tool.
	- The Results of the DQ Checkpoint Reviews.	- The entity must attach a report clarifying the review/audit results of the DQ Checkpoints including the following, at a minimum: - A log containing the detected DQ issues. - A remediation plan for the detected DQ issues.
Level 4: Managed	- Trends from the DQ Monitoring Activities with Pre-defined KPIs.	- The entity must attach an updated report, approved by the entity's authority holder on measuring the effectiveness of implementing DQ monitoring activities based on pre-defined and identified KPIs and indicator cards, including the following, at a minimum: - The number of DQ issues reported based on the established & implemented DQ Rules. - The number of DQ issues reported by the Data Catalog users. - The number of the DQ Rules deployed. - Each indicator card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator.

Checklist – Data Quality Domain		
DQ.MQ.3	Has the entity established and implemented practices to monitor and report the entity's Data Quality (DQ) status?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The Continuous Improvement Report on the DQ Monitoring and Reporting Practices.	- The entity must attach an updated & approved report presenting continuous improvement of DQ monitoring and reporting practices based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: - Reviews conducted. - Results of each review. - Improvements implemented (with supporting documents).

Checklist – Data Quality Domain		
DQ.MQ.4	Has the entity developed Data Quality (DQ) standards, provided definitions for its datasets, and published / uploaded the definitions on the National Data Catalog (NDC)?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- The Existing List of Data Standards and Data Definitions.	- The entity must attach an updated & approved report listing the current DQ standards and explaining the Data definitions.
Level 2: Defined	- The Developed Data Standards for Data Elements.	- The entity must attach an updated & approved report clarifying the Standards developed for the Data Elements.
	- The Identified Metadata with their Definitions.	- The entity must attach an updated & approved report clarifying the identified Metadata with their definitions.

Checklist – Data Quality Domain		
DQ.MQ.4	Has the entity developed Data Quality (DQ) standards, provided definitions for its datasets, and published / uploaded the definitions on the National Data Catalog (NDC)?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Identified Datasets to be Published on the National Data Catalog (NDC).	- The entity must attach an updated & approved report showing the identified datasets to be published on the National Data Catalog (NDC).
Level 3: Activated	- A Report about the Data Standards & the Data Definitions which the Entity Uploaded on the NDC.	- The entity must attach an updated & approved report proving that the entity's Data Standards & Data Definitions have been published on the National Data Catalog (NDC).
	- The Entity-Specific List of Applied Data Definitions and Applied Data Standards.	- The entity must attach an updated & approved report listing the approved entity specific definitions & Data standards.
Level 4: Managed	- A Monitoring Report for the Data Definitions and Data Standardization with Pre-defined KPIs.	- The entity must attach an updated report, approved by the entity's authority holder on measuring the effectiveness of implementing monitoring Data Definitions and Standardizations based on pre-defined and identified KPIs and indicator cards, including the following, at a minimum: • The percentage of defined Data Elements. • The percentage of business Metadata attributes which are defined and published to the NDC. • The percentage of technical Metadata attributes which are defined and published on the NDC. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target).

Checklist – Data Quality Domain		
DQ.MQ.4	Has the entity developed Data Quality (DQ) standards, provided definitions for its datasets, and published / uploaded the definitions on the National Data Catalog (NDC)?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The continuous Improvement Report for Optimizing the Data Standards and Definitions within the Entity and on the NDC.	- The entity must attach an updated & approved report presenting regular reviews and continuous improvements of Data Standards & Data Definitions both: within the entity and on the National Data Catalog (NDC) based on the results of the KPI measurements and relevant updates and developments in the domain, including the following, at a minimum: - The documents of the periodic reviews & documented results of the Data Standards & Data Definitions. - The continuous improvement mechanisms of the Data Standards & Data Definitions. - Improvements implemented (with supporting documents).

8.2.4.Data Operations Domain

Checklist – Data Operations Domain		
DO.MQ.1	Has the entity developed and implemented a plan to manage and satisfy the needs of Data Operations, data storage and data retention?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- The Approved Initial Data Operations and Storage Plan.	- The entity must attach the initial Data Operations and Storage Plan including the following, at a minimum: • A roadmap that includes the activities and milestones. • The assignment of the required resources & budget allocation.
Level 2: Defined	- The Developed and Approved Data Operations and Storage Plan.	- The entity must attach the developed Data Operations and Storage Plan, approved by the entity's authority holder including the following, at a minimum: • A roadmap that includes activities and milestones to implement Data Operations and Storage Plan within the entity. The activities must include what is necessary to achieve the domain's specifications, at a minimum. • The assignment of the required resources & budget allocation to manage the activities included in the roadmap.
	- The Information Systems Priority List.	- The entity must attach a prioritized lists of the information systems based on: • Their criticality to the business progress to ensure business continuity. • The system recovery order in the Disaster Recovery (DR) plan.
	- The Developed and Approved Policies for Data Operations, Storage, Retention and Business Continuity.	- The entity must attach a report on the Policies which are approved for Data Operations, storage, retention, and business continuity, including the following, at a minimum: • Storage conditions which ensure data protection in disaster events. • Data retention periods based on data type, Data Classification (DC) level, Data value for/in the business, and legal requirements.

Checklist – Data Operations Domain		
DO.MQ.1	Has the entity developed and implemented a plan to manage and satisfy the needs of Data Operations, data storage and data retention?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The disposal and destruction rules based on the data type and classification level. - The required actions in the event of an accidental permanent loss of data. - Each Policy document includes the following at a minimum: - Policy title / name. - Policy owner. - Release date. - Version number. - Version history. - Objective. - Identified stakeholders, e.g.: Target audience. - Communications process. - Monitoring procedure. - Document control (Preparation, review, approval). - Policy Statement. - Roles & responsibilities. - Terminology. - Scope of work. - Activation mechanisms. - Approval. - References.
	- The Periodic Forecasting Plan for Storage Capacity.	- The entity must attach a periodic forecast report on proactive planning to satisfy the expected storage capacity requirements, including the following, at a minimum: - Previous (historical) data storage capacities used. - Performance Evaluation of the entity's applications and needs. - A list of upcoming applications to be developed and built for the entity.
	- The Database Technology Evaluation Process and Selection Criteria.	- The entity must attach the Database Technology Evaluation Process and Selection Criteria including the following, at a minimum: - The Total Cost of Ownership (TCO) including, at least: licensing, support, training, and hardware.

Checklist – Data Operations Domain		
DO.MQ.1	Has the entity developed and implemented a plan to manage and satisfy the needs of Data Operations, data storage and data retention?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The availability of resources skilled in these technological solutions, both internally and in the job market. - The presence of software tools related to the Database technologies being evaluated in the entity. - Volume and velocity limits of the utilized technologies. - Reliability provided by the utilized technologies. - Scalability of each technology. - Security controls provided by the utilized technologies.
Level 3: Activated	- The Data Operations and Storage plan with implementation status report.	- The entity must attach a report of Data Operations and Storage Plans implementation status, including the following, at a minimum: Initiatives and projects status: Identifying the status of each initiative or project (started, in progress, completed, or delayed), along with clarification of any delays or challenges. Progress percentages: Providing the progress percentages of activities and milestones in the plan and roadmap, with clear details on the actual activities that have been completed. Supporting evidence: Attaching proof of achieved progress/completion, such as reports, photos, documents, or meeting minutes that support the implementation status.
	- The Storage Trend Forecast Document.	- The entity must attach a report clarifying the expected storage capacity, including the following, at a minimum: - Forecasting the entity's future needs of data storage capacity. - Estimating budgets for future purchases of data storage space.
	- The Database Technology Evaluation Report.	- The entity must attach a database technology assessment report including the following, at a minimum: - The performance of database technologies. - The availability of technical support for the current version of each database technology. - Technical support availability for software tools and operating systems of the databases.

Checklist – Data Operations Domain

DO.MQ.1	Has the entity developed and implemented a plan to manage and satisfy the needs of Data Operations, data storage and data retention?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Document on the Entity's Application Performance Assessment.	- The entity must attach an evaluation report on the performance of the entity's applications, including the following, at a minimum: - The number of transactions by each application used in the entity. - The percentage % of application utilization to perform the entity's work in an automated manner. - Availability – Users Accessibility to the entity's applications.
	- The Entity's Applications Development Roadmap with the Status Report on the Implementations.	- The entity must attach a roadmap document for the upcoming applications to be developed and a report on their development statuses, including the following, at a minimum: - The activities and milestones. - Application development prioritization. - Each application's development status.
	- The Budget Estimations of the Procurement Transactions of the Future Storage Needs.	- The entity must attach a report clarifying the estimated budgets for future procurements of data storage processes.
	- The Data Operations Orchestration Document.	- The entity must attach a document on Data Operations Orchestration, including assigning teams to operate and maintain systems data, plus to process and analyze data.
Level 4: Managed	- The Monitoring Report with Pre-defined Key Performance Indicators (KPIs) for the Implementation Progress and Effectiveness of the Data Operations Plan.	- The entity must attach an updated report, approved by the entity's authority holder to monitor the progress and effectiveness of implementing the data storage operation plan based on pre-defined and indicated KPIs and Indicator Cards, including: - The percentage of data storage capacity. - The percentage of total capacity utilized. - The utilization rates for each type of database. - The percentage of capacity used for backups. - The number of executed data transactions. - The average query execution time. - Each indicator card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator.

Checklist – Data Operations Domain

DO.MQ.1	Has the entity developed and implemented a plan to manage and satisfy the needs of Data Operations, data storage and data retention?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The Continuous Improvement Report on the Practices of Data Operations, Storage, and Retention.	- The entity must attach an updated report, approved by the entity's authority holder demonstrating continuous improvement of the data storage domain plan based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: - Reviews conducted. - Results of each review. - Improvements implemented (with supporting documents).

Checklist – Data Operations Domain		
DO.MQ.2	Does the entity have in place a defined methodology, processes and Standard Operating Procedures (SOPs) for database operations?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- Evidences of Data Operations Done within the Entity.	- The entity must attach evidences of the database operations performed by the entity (e-mails, screenshots).
Level 2: Defined	- The Process Documentation of the Detailed Practices of Data Operations, Including: A. Database Monitoring.	The entity must attach the overall Process of the Detailed Practices of Database Monitoring including: The process for monitoring and reporting database performance on regular basis.
	B. Database Access Control.	The entity must attach the Detailed process for providing the entity's employees access to the databases.
	C. Storage Configuration Management.	The entity must attach the detailed Practices of Storage Configuration Management including at a minimum: - Configuration identification. - Configuration change control. - Configuration status accounting. - Configuration audits.
	D. DBMS Versioning Mechanism.	The entity must attach the overall Process of the Detailed Practices of DBMS Versioning / Updating Mechanism Covering: - The Management Plan of Updated Releases / Versions. - The Strategy Including Analysis and Rationale.
	E. The Database Performance Service Level Agreements and Operational Level Agreements (SLAs & OLAs).	The entity must attach the process for defining Database Performance Service Level Agreements and Operational Level Agreements (SLAs & OLAs).

Checklist – Data Operations Domain		
DO.MQ.2	Does the entity have in place a defined methodology, processes and Standard Operating Procedures (SOPs) for database operations?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 3: Activated	- The Database Monitoring Status Report.	- The entity must attach a monitoring status report on database performance, including the following, at a minimum: • Capacity – The size of the unused storage. • Availability – Users' accessibility to the entity's databases, as & when needed. • Queries Execution Performance – Query execution times, durations and errors. • Tracking Changes – Tracking database changes for root cause analysis, as & when needed.
	- The Data Operations Operating Model.	- The entity must attach the approved Operational Model of Database Operations, including the following, at a minimum: • The teams' roles and responsibilities. • The procedures and practices of Database Operations management. • The technologies used to support Database Operations.
	- Evidences of Agreements (SLAs and OLAs).	- The entity must attach a report on database performance agreements, e.g.: Service Level Agreements (SLAs) and Operational Level Agreements (OLAs); including the following, at a minimum: • The timeframe of making the database available for users. • The maximum time allowed to complete electronic transactions on a specific application. • Each agreement must clarify the escalation procedures to be followed when the agreement is violated.
Level 4: Managed	- The Monitoring Report with Pre-defined KPIs for Database Operations Management.	- The entity must attach an updated report, approved by the entity's authority holder on monitoring Database Operations Management based on pre-defined and identified KPIs and indicator cards. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description.

Checklist – Data Operations Domain		
DO.MQ.2	Does the entity have in place a defined methodology, processes and Standard Operating Procedures (SOPs) for database operations?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The Continuous Improvement Report on the Implemented Practices and Processes of Data Operations and Storage.	- The entity must attach the continuous improvement report of the implemented practices and applied processes for operating and storing data procedures/processes, based on the results of the KPI measurements and relevant updates and developments in the domain, containing the following, at a minimum: - Evidence of the data processes and storage automation. - Review and results documentation: Periodic review and result documentation for data processes and storage. - Continuous improvement mechanisms: Continuous improvement mechanisms for data processes and storage.
	- The Knowledgebase document.	The entity must attach a Knowledgebase document including the following, at a minimum:

Checklist – Data Operations Domain		
DO.MQ.2	Does the entity have in place a defined methodology, processes and Standard Operating Procedures (SOPs) for database operations?	
Levels	Acceptance Evidence	Acceptance Criteria
		- All lessons learnt, test / trial cases and user stories. - The log of errors and issues. - The solutions of the recorded errors and issues.

Checklist – Data Operations Domain		
DO.MQ.3	Does the entity have in place, practices and processes for Business Continuity such as backup and disaster recovery (DR) and a defined Business Continuity Plan (BCP) for the data?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- Evidences of Data Storage Backup Instruction Documents.	- The entity must attach a sample document of the data storage backup instructions (e-mail, guide / manual).
Level 2: Defined	- The Developed Processes and Practices for Data Storage Backups and Recovery.	- The entity must attach the process and practices developed for the "Data Storage Backup" and "Data Backup Recovery", including the following, at a minimum: - Defining and determining the backup frequency of each information system. - Scope of backup for each information system including the scope of Data and the scope of database transaction logs. - Location of backup files including a storage medium and a physical location.

Checklist – Data Operations Domain		
DO.MQ.3	Does the entity have in place, practices and processes for Business Continuity such as backup and disaster recovery (DR) and a defined Business Continuity Plan (BCP) for the data?	
Levels	Acceptance Evidence	Acceptance Criteria
		Periodic validations of backup completions using system copies in non-production environments.
	- The Business Continuity Plan (BCP) and Processes.	- The entity must attach the Business Continuity Plan (BCP) and Processes including the following, at a minimum: - Risk assessment and business impact analysis. - Job roles and responsibilities. - Alternative work locations. - The infrastructure. - Incident management. - The communication mechanisms of the continuity procedures to notify the relevant stakeholders, e.g.: Employees and customers. - Periodic training courses with scenario-based trial simulations to evaluate the response and identify areas for improvement.
	- The Disaster Recovery (DR) Processes and Plan.	The entity must attach: - The Disaster Recovery (DR) Processes and Plan including, at a minimum, the following: - A prioritized list of information systems defining their recovery order. - Assigning the roles responsible for addressing/handling incident cases and responding. - Defining and specifying the procedural actions to be taken to activate a response to each incident through the system. - Defining and specifying the procedural actions to be taken to reduce the damage and mitigate the incident consequences on the entity's critical operations. - Definition & identification of Recovery Point Objectives (RPO) (A maximum targeted period within which data might be lost without causing damage to the business) for each information system covered in the plan. - Definition of Recovery Time Objectives (RTO) (A maximum targeted duration of time within which the database can be down without causing damage to the business) for each information system covered in the plan - Definition of recovery/restoration activities.

Checklist – Data Operations Domain

DO.MQ.3	Does the entity have in place, practices and processes for Business Continuity such as backup and disaster recovery (DR) and a defined Business Continuity Plan (BCP) for the data?	
Levels	Acceptance Evidence	Acceptance Criteria
		Periodic training courses with scenario-based trial simulations to evaluate the response and identify areas for improvement.
	A Document of Actions Required to Implement Database Changes and Rollbacks.	The entity must attach a document explaining the definitions of the measures and the procedural action steps to be taken to implement the changes on each database or to rollback / undo the changes as & when needed.
Level 3: Activated	The Technical Design Document.	- The entity must attach the Technical Design document including the following, at a minimum: - Accurate information about the technical infrastructure of the main location and the Disaster Recovery (DR) location. - The processes and procedures which are required for data recovery. - System architecture, including hardware, software, and network structure. - Tasks and responsibilities of the technical team responsible for DR. - Testing and maintenance procedures of the DR processes.
	The BCP Run Report.	- The entity must attach the BCP Run Report, i.e., the output doc after BCP execution, explaining the results, recommendations, etc. which ensure the continuous availability of critical business functions during adverse / damaging incidents. The following must be included, at a minimum: - The implementation status of the BCP, practices, and processes.
	The DR Plan Run Report.	- The entity must attach the DR Plan Run Report, i.e., the output doc after BCP execution, explaining the results, recommendations, etc. which ensure the continuous availability of critical business functions during adverse/damaging incidents. The following must be included, at a minimum: - The implementation status of the DR Plan, practices, and processes.
	The Change Request form for Data Change in the Production Environment.	- The entity must attach the approved Change Request form/template used for requesting a data change in the production environment. Including the following, at a minimum: - Change requestor details.

Checklist – Data Operations Domain		
DO.MQ.3	Does the entity have in place, practices and processes for Business Continuity such as backup and disaster recovery (DR) and a defined Business Continuity Plan (BCP) for the data?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Description of the requested change. - Reason for the change. - Impact of the change on (the current system, daily operations, end-user). - Implementation steps. - Backup plan. - Testing period (the period for testing the change before final approval). - Rollback plan. - Approval from the entity's authority holder.
	- The Production Data Access Control Document.	- The entity must attach the Access Control document of data in the production environments (based on the authorizations matrix and according to job roles), including the following, at a minimum: - The change requests initiating the process. - Definition and identification of procedural actions to be taken for a controlled implementation of changes in the databases. - Definition and identification of procedural actions to be taken for rollback / reversing the changes in cases of identified issues.

Checklist – Data Operations Domain		
DO.MQ.3	Does the entity have in place, practices and processes for Business Continuity such as backup and disaster recovery (DR) and a defined Business Continuity Plan (BCP) for the data?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 4: Managed	- The Monitoring Report with Pre-defined KPIs for the Business Continuity (BCP) and Disaster Recovery (DR).	- The entity must attach an updated report approved by the entity's authority holder on monitoring the effectiveness of the Business Continuity Plan (BCP) and Disaster Recovery (DR) based on pre-defined and identified KPIs and indicator cards. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The Continuous Improvement Report on the Business Continuity Plan (BCP).	- The entity must attach the continuous improvement report for BCP based on the results of the KPI measurements and relevant updates and developments in the domain, including the following implemented improvements, at a minimum: • BCP.

Checklist – Data Operations Domain		
DO.MQ.3	Does the entity have in place, practices and processes for Business Continuity such as backup and disaster recovery (DR) and a defined Business Continuity Plan (BCP) for the data?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Processes for production environment authorization access control. - Processes for Data backup and recovery. - DR plan. - The continuous improvement report must include the following, at a minimum: - The documents of reviews & results: Periodic review and result documentation for data processes and storage. - The continuous improvement mechanisms: Mechanisms for the continuous improvement of data processes and storage.

8.2.5.Document and Content Management Domain

Checklist – Document and Content Management Domain		
DCM.MQ.1	Has the entity developed a Document and Content Management (DCM) plan and a Digitization plan to manage the implementation of paperless management activities?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- Evidences of Existing DCM Activities.	- Evidences must be attached proving the existence of DCM activities, including what supports practicing a DCM activity such as: - Copies / screenshots of e-mails. - Copies / screenshots of documents. - Screenshots of systems / tools.
Level 2: Defined	- The DCM Plan.	- The entity must attach a recent DCM plan, approved by the entity's authority holder that includes the following, at a minimum: - A roadmap that includes the activities and milestones for the entity's implementation of Documents and Content Management activities. The activities shall incorporate what is needed to achieve this Domain's specifications, at a minimum. - The assignment of required resources & budget allocation to manage and implement activities included in the roadmap.
	- The DCM Digitization Plan.	- A report must be attached containing a recent DCM Digitization Plan, approved by the entity's authority holder, and the implementation status with the necessary details as follows, at a minimum: - Roadmap with the activities and key milestones for the migration of the entity's existing paper-based documents to the electronic format. The activities shall incorporate what is needed to achieve this Domain's specifications, at a minimum. - Roadmap with the activities and key milestones for the implementation of initiatives focused on eliminating the creation of paper-based documents in the entity and replacing them with electronic documents. The activities shall incorporate what is needed to achieve this domain's specifications, at a minimum.

Checklist – Document and Content Management Domain		
DCM.MQ.1	Has the entity developed a Document and Content Management (DCM) plan and a Digitization plan to manage the implementation of paperless management activities?	
Levels	Acceptance Evidence	Acceptance Criteria
		The assignment of required resources & budget allocation to manage and implement activities included in the roadmap.
	The Developed Prioritization Process for Documents and Content.	- The Prioritization Process of Documents and Content must include the following, at a minimum: - The definition of “Data Prioritization”. - The prioritization matrix. - The identification and definition of DCM procedures. - The ranked list of prioritized document workflows.
	The Identified DCM Processes / Procedures.	The entity must identify the key processes that will represent the workflow of documents in the Document Management System and prioritize them to implement an automated Document Management System within the entity.
	The Ranked List of Prioritized Document Workflows to be Implemented.	- The entity must attach a report clarifying a ranked list of tasks for each prioritized Workflow of Documents, including: - The definition and rating of the workflows based on the level of importance and impact on business operations. - The tasks of each prioritized Workflow based on the compliance requirements, risk factors, and operational needs. - A clear implementation roadmap for each Workflow including the timelines and resource assignments.
	The Developed DCM Training Plan.	- The entity must attach the developed DCM training plan, including: - The target audience groups identified in the training plan, such as employees, managers, and IT staff. - The developed training curricula, including presentations, handouts and online resources, designed / customized specifically to satisfy the identified & defined needs. - The training delivery staff’s assigned responsibilities, including trainers or facilitators. - The training schedule. - The training plan must be valid and approved by the entity’s authority holder
Level 3: Activated	The DCM Plan Implementation Status Report.	- The entity must attach a report of the DCM plan implementation status and roadmap, including the following, at a minimum: Initiatives and projects status: Identifying the status of each initiative or project (started, in progress, completed, or delayed), along with clarification of any delays or challenges.

Checklist – Document and Content Management Domain		
DCM.MQ.1	Has the entity developed a Document and Content Management (DCM) plan and a Digitization plan to manage the implementation of paperless management activities?	
Levels	Acceptance Evidence	Acceptance Criteria
		Progress percentages: Providing the progress percentages of activities and milestones in the plan and roadmap, with clear details on the actual activities that have been completed. Supporting evidence: Attaching proof of achieved progress/completion, such as reports, photos, documents, or meeting minutes that support the implementation status.
	- The Digitization Plan Implementation Status Report.	- The entity must attach a report of the Digitization Plan implementation status and roadmap, including the following, at a minimum: Initiatives and projects status: Identifying the status of each initiative or project (started, in progress, completed, or delayed), along with clarification of any delays or challenges. Progress percentages: Providing the progress percentages of activities and milestones in the plan and roadmap, with clear details on the actual activities that have been completed. Supporting evidence: Attaching proof of achieved progress/completion, such as reports, photos, documents, or meeting minutes that support the implementation status.
	- The List of Prioritized Documents for Digitization.	A report must be attached clarifying the prioritized list of documents to be digitized based on the Inventory of Data Elements within the entity.
	- The DCM Roles and Responsibilities.	The entity must attach job titles along with the roles and responsibilities for each position required to perform DCM tasks, approved by the entity's authority holder.
	- The DCM Training Plan Implementation Status Report.	- The DCM Training Plan Implementation status report must be attached including the following, at a minimum: - The objectives of the training program with the topics covering: - Introduction of the DCM Policies. - Introductory and advanced tutorials about DCM systems used by the entity and their functionalities. - The dates and implementation status, as well as attaching supporting evidence of implementation.
Level 4: Managed	- The Monitoring Reports with Pre-defined KPIs for the Implementation of the DCM Plan & the DCM Digitization Plan.	- The entity must attach an updated report, approved by the entity's authority holder on measuring the implementing DCM Plan and DCM Digitization Plan based on pre-defined and identified KPIs and indicator cards, covering: - The Monitoring Report with approved & pre-defined KPIs for the Implementation of the DCM Plan, with the Indicator Card(s) attached.

Checklist – Document and Content Management Domain		
DCM.MQ.1	Has the entity developed a Document and Content Management (DCM) plan and a Digitization plan to manage the implementation of paperless management activities?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The Monitoring Report with approved & pre-defined KPIs for the Implementation of the Digitization Plan, with the Indicator Card(s) attached. - Each indicator card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator value
Level 5: Pioneer	The Continuous Improvement Report of the DCM and Digitization Plans.	- The entity must attach an updated report, approved by the entity's authority holder presenting continuous improvement of DCM & Digitization Plans based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: - Reviews conducted. - Results of each review. - Improvements implemented (with supporting documents).

Checklist – Document and Content Management Domain		
DCM.MQ.2	Has the entity implemented policies and processes for Document and Content Management (DCM) including: Backup & Recovery, Retention & Disposal, Document & Content Access Approval, and Metadata Publishing?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	- No required documents
Level 1: Establishing	- Evidences of Processes for Retaining & Disposing of Documents.	- Evidences must be attached, covering the Processes of Document Retention and Disposal, including what supports practicing each procedure / process such as: • Copies / screenshots of e-mails. • Copies / screenshots of documents. • Screenshots of systems / tools.
Level 2: Defined	- The Developed Policy Document for the DCM Lifecycle.	- Across the DCM Lifecycle, the entity must attach the developed Policies for each of the following, at a minimum: • The Naming Convention Policies. • Policies for assigning classification levels to documents. • The Access Approval Policies. • The Backup & Recovery Policies. • The Retention & Disposal Policies. Every Policy's document must include, the following, at a minimum: • Policy Name. • Policy Owner. • Release date. • Version number. • Document control (Preparation, review, approval). • Version history. • Terminology. • Goal. • Scope of work. • Principles • Policy Statement. • Job roles & responsibilities. • Related Policies. • References.

Checklist – Document and Content Management Domain		
DCM.MQ.2	Has the entity implemented policies and processes for Document and Content Management (DCM) including: Backup & Recovery, Retention & Disposal, Document & Content Access Approval, and Metadata Publishing?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Developed DCM Backup & Recovery Procedures.	- The entity must attach reports showing evidence that the entity has included the Document and Content Management Systems within its overall backup and recovery plan for DCM Backup & Recovery.
	- The Developed DCM Retention & Disposal Procedures.	- The entity must attach reports containing the documentations of the developed DCM Retention & Disposal Processes/ Procedures.
	- The Developed DCM Role-Based Access Approval Procedures.	- The entity must attach reports containing the documentations of the developed DCM Access Approval & Role-Based Access Authorization Processes.
	- The Developed DCM Metadata Publishing Procedures.	- The entity must attach reports containing the documentations of the developed processes for the following: • Publishing the Metadata of Documents & Contents. • Classifying Documents & Contents.
Level 3: Activated	- The Implemented Workflow for the DCM Retention & Disposal Process.	- Evidence must be attached for the workflow performed for the Retention & Disposal process. This shall include: • Evidence of handover of documents to the entity's archival facility. • Evidence of physical destruction of documents, including overwriting and a secure deletion.
	- The Implemented Workflow for the DCM Access Approval Process.	- Evidence must be attached for the workflow performed for the Access Authorization Approval process based on job roles & job tasks (A copy of the work procedure steps).
	- Evidences of Document Transfers to the Archival Facility (Archival Register).	- Evidences must be attached to prove transferring documents to the entity's Archival Facility / Archives Unit. (Registering the archive in a system), e.g.: Copies of Archived Documents.
	- The Documents Disposal Register.	- Evidences must be attached to prove the existence of a Register for logging the Disposal of Documents (A copy of the Documents Disposal Register).
	- The Access Rights Documentation.	- The entity must attach the Access Rights Documentation including the following, at a minimum: • The mechanism of accessing documents and contents clarifying the dependence of the role and job tasks. • The identified Access Groups based on Data Classification Domain Standards & Controls.
	- The Report on Document & Content Metadata Publishing.	- The entity must attach a report on Publishing Metadata of Documents & Contents, including the following, at a minimum:

Checklist – Document and Content Management Domain		
DCM.MQ.2	Has the entity implemented policies and processes for Document and Content Management (DCM) including: Backup & Recovery, Retention & Disposal, Document & Content Access Approval, and Metadata Publishing?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The Metadata Standards. - The Forms / Templates. - The Data Catalog Integration document.
Level 4: Managed	The Monitoring Report with Pre-defined Key Performance Indicators (KPIs) of the DCM Processes Aligned with the Policies.	- The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of DCM processes aligned with the policies. This should be based on pre-defined and identified KPIs and indicator cards, including the following, at a minimum: - The size / volume of the entity's Documents stored in the entity's Document Management System (DMS). - The number of users of the entity's Document Management System (DMS). - The percentage % of the paper-based documents transformed into electronic formats. - Each indicator card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values

Checklist – Document and Content Management Domain		
DCM.MQ.2	Has the entity implemented policies and processes for Document and Content Management (DCM) including: Backup & Recovery, Retention & Disposal, Document & Content Access Approval, and Metadata Publishing?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 5: Pioneer	- The Continuous Improvement Report on the DCM Processes and Practices.	- The entity must attach the continuous improvement report of the DCM processes and practices, based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: • Evidence of DCM processes and practices automation. • Review and results documentation: Periodic review and result documentation for DCM processes and practices. • Continuous improvement mechanisms: Continuous improvement mechanisms for DCM processes and practices.

Checklist – Document and Content Management Domain		
DCM.MQ.3	Has the entity implemented a tool to support Document and Content Management (DCM) processes including Digitization Management Implementation?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- Evidences of Document Storage / Retention & Disposal Activities.	- The entity must attach a report on the current activities related to document storage, document retention, and document disposal, including one of the following to support practicing each activity, e.g.: • Copies / screenshots of e-mails. • Copies / screenshots of documents. • Screenshots of systems / tools.
Level 2: Defined	- The Documented DCM Tool Requirements.	- The entity must attach the documented DCM Tool requirements, including the following, at a minimum: • The functional requirements of the tool. • The non-functional requirements of the tool. • The tool's use case template / form.
Level 3: Activated	- The Implemented Tool for DCM.	- The entity must attach evidences that the implemented DCM tool includes the following, at a minimum:

Checklist – Document and Content Management Domain		
DCM.MQ.3	Has the entity implemented a tool to support Document and Content Management (DCM) processes including Digitization Management implementation?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Document Management System - an application used to capture, store and manage documents in an electronic format (electronic documents and digital media). The selected DMS tool shall provide, at minimum, the following capabilities: - Storage of documents. - OCR (Optical Character Recognition) functionality to analyze imported images. - Indexing of documents. - Versioning of documents including tracking of the history of changes. - Secured access to documents. - Global search and discovery on the registered documents. - Documents workflows development. - Web Content Management System - an application used to store and manage website Content used by the entity's portals and internet sites. - Collaboration tools – applications providing users with platform to collaborate real-time on electronic documents, communicate using chat and track changes in the documents.
	- The Record of Digitized Documents.	- The entity must attach an evidence of the number of Digitized Documents (A copy of the Record of Digitized Documents).
	- The List of Approved Users.	- The entity must attach a list of the approved users of the DCM system/tool and their roles (Screenshots showing users and their roles).
Level 4: Managed	- The Monitoring Report on the Implemented Tool with Pre-defined Key Performance Indicators (KPIs).	- The entity must attach an updated report, approved by the entity's authority holder on monitoring the implemented tool based on pre-defined and identified KPIs and indicator cards. - Each indicator card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value.

Checklist – Document and Content Management Domain		
DCM.MQ.3	Has the entity implemented a tool to support Document and Content Management (DCM) processes including Digitization Management implementation?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The Continuous Improvement Report on the DCM Solution / Tool Design and DCM Practices.	- The entity must attach the continuous improvement report regularly on the implemented tool performance, based on the results of the KPI measurements and relevant updates and developments in the domain, containing the following, at a minimum: - Review and results documentation: Periodic review and result documentation for the implemented tool performance. - Continuous improvement mechanisms: Continuous improvement mechanisms for the implemented tool performance.

8.2.6.Data Architecture and Modelling Domain

Checklist – Data Architecture and Modelling Domain		
DAM.MQ.1	Has the entity developed and implemented a plan to improve its Data Architecture Capabilities?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents

Checklist – Data Architecture and Modelling Domain		
DAM.MQ.1	Has the entity developed and implemented a plan to improve its Data Architecture Capabilities?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 1: Establishing	- The existing DAM Domain related practices.	- The entity must attach a report clarifying the current DAM practices.
Level 2: Defined	- The Approved DAM Plan.	- A recent DAM plan, approved by the entity's authority holder must include the following, at a minimum: - Roadmap with the activities & milestones for the Target State Data Architecture. The activities shall incorporate what is needed to achieve this Domain's specifications, at a minimum. - The assignment of the required resources & budget to manage the implementation of the Target State Data Architecture.
	- The Approved Current State Data Architecture & the Existing Technical Architecture.	- The entity must attach a report on the Current State Data Architecture and the Technical Architecture to support the development of the Target Architecture. The Current Data Architecture & the existing Technical Architecture shall cover, at a minimum: - A data model at the conceptual, logical and physical levels. - The current processes used in conducting business processes & decision making. - The Key System Components – The current essential applications, data storages, data processing platforms, and data analytics solutions used in key processes. - Data flow and data lineage.
	- The Approved Target State Data Architecture.	- The entity must attach the Target Data Architecture including the following, at a minimum: - A data model at the conceptual, logical and physical levels. - The targeted processes used in conducting business processes & decision making. - The Key System Components – The targeted essential applications, data storages, data processing platforms, and data analytics solutions used in key processes. - Data flow and data lineage.
	- The Future State Gap Assessment.	- The entity must attach a report on the Future-State Gap Assessment including the following, at a minimum: An analysis of the gaps between the Current Data Architecture and the Target Data Architecture as one of the inputs for the DAM plan.

Checklist – Data Architecture and Modelling Domain

DAM.MQ.1	Has the entity developed and implemented a plan to improve its Data Architecture Capabilities?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Approved Enterprise Architecture Framework.	- The entity must attach the Enterprise Architecture (EA) Framework and the general Model of the EA components so that the Government entity would have a comprehensive business & IT blueprint that's linked & aligned with the entity's strategic objectives.
	- The DAM Policy.	- The entity must attach the DAM Policies, approved by the entity's authority holder including the following for each policy, at a minimum: • Policy Name. • Release Date. • Release Number. • Document Control (Preparation, Review, Approval). • Version History. • Terminologies. • Goal. • Scope of Work. • Roles & Responsibilities. • References. • Policy Owner. • Policy Statement including the following, at a minimum: • The Target Data Architecture shall address the strategic requirements defined within the entity's Data Management & Personal Data Protection (DM & PDP) Strategy. • The Target Data Architecture shall be mapped with the overall Enterprise Architecture (EA). • The Target Data Architecture shall adopt a popular Enterprise Architecture Framework, e.g., TOGAF, Zachmann. • The regular mechanisms of monitoring & updating Data Models.
Level 3: Activated	- The DAM Plan Implementation Progress Report.	- The entity must attach a report clarifying the implementation status including the following, at a minimum: • The achievement percentages of the initiatives & projects included in the DAM Implementation Plan.
	- The EA Framework Implementation Report.	- The entity must prove the application of the approved EA Framework by attaching samples from the used EA tool or the National EA Certificate of Approval.

Checklist – Data Architecture and Modelling Domain		
DAM.MQ.1	Has the entity developed and implemented a plan to improve its Data Architecture Capabilities?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 4: Managed	- The Monitoring Report of the DAM Plan & Activities Implementation with Pre-defined KPIs.	- The entity must attach an updated report, approved by the entity's authority holder to measure the effectiveness of implementing the DAM plan in tracking the progress achieved in transforming the current data architecture into the target architecture, based on pre-defined and identified KPIs and indicator cards, including the following, at a minimum: - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values

Checklist – Data Architecture and Modelling Domain		
DAM.MQ.1	Has the entity developed and implemented a plan to improve its Data Architecture Capabilities?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 5: Pioneer	- The Data Architecture Plan's Continuous Improvement Report.	- The entity must attach a report showing that the entity identified, implemented, and is monitoring the Data Architecture Plan's continuous improvement mechanisms, based on the results of the KPI measurements and relevant updates and developments in the domain. The report must contain the following, at a minimum: • The Documentation of the periodic Data Architecture reviews and the documented results. • The continuous improvement mechanisms.
	- The Architecture Change Management Process.	- The entity must attach a document clarifying a specific Architecture Change Management Process for reviewing, approving and implementing changes in the Current & Target Data Architectures. The Architecture Change Scope shall include the following, at a minimum: • The requests for new DAM initiatives. • The modifications on the Current State Architecture documents of the existing initiatives.
	- The Change Control Document.	- The entity must attach a document clarifying the Change Control Process to be used in changing the Current & Target Data Architectures. The document shall include the following, at a minimum: • The scope of change. • The impact assessment of the change. • The procedures of the change. • The roles & responsibilities. • The data of change approvals. • The data of the change requester.
	- The Data Architecture Checkpoints Report.	- The entity must attach a report showing that the entity incorporated Data Architecture Checkpoints in the Software Development Lifecycle (SDLC) processes. The Checkpoints shall include the following, at a minimum: • Investigating the possibilities of reusing the existing Data Architecture components to address the business requirements. • Validating the conformance of the created Data Models with the entity's Enterprise Data Model. • Verifying if the project implies any change required to be done on the entity's overall Enterprise Data Model.

Checklist – Data Architecture and Modelling Domain		
DAM.MQ.2	Has the entity developed and implemented practices for Data Architecture & Modelling (DAM) activities (including Data Flows, Data Models and Governance considerations)?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	- No required documents
Level 1: Establishing	- The Current Data Flows and Data Models Activities.	- The entity must attach the following, at a minimum: • Proof of the current processes followed to manage the Data Flow & DAM Practices. • Documents which clarify the current (Conceptual & Logical) Data Models. • Documents which clarify the Data Lineages (of Data Flows) being aligned with business requirements.
Level 2: Defined	- A document containing the Approved Business Processes on the Data Architecture and any Related Data Flow.	The entity must attach a document clarifying the conducted Business procedures on the Data Architecture, identifying the roles & responsibilities to ensure compliance with DAM Policies and effective & systematic achievements of Data Architecture activities.
	- A document containing the Big Data Considerations Including the Data Lake Requirements.	- The entity must attach a document specifying the requirements for developing a Data Storage/Lake Environment using a neutral Big Data Reference Architecture Framework (e.g., NIST) and incorporating Big Data architecture components into its overall target Data Architecture design. The Data Storage/Lake requirements shall address the following, at a minimum: • Ingest – Ingesting and converting semi/partially structured & unstructured datasets into a structured form. • Infrastructure – Networking, computing and storage requirements needed to handle large, diverse formats of data. • Platform – A distributed storage solution providing distributed computing / processing capabilities.
	- A document containing the Data Processing Considerations Including the Partitioning Strategy.	- The entity must attach a document specifying data processing considerations including the following, at a minimum: • A partitioning strategy for its Target State Data Architecture for efficient processing of various data volumes, data variety & data velocity. • The partitioning strategy coverage of both real time and batch processing operations.

Checklist – Data Architecture and Modelling Domain		
DAM.MQ.2	Has the entity developed and implemented practices for Data Architecture & Modelling (DAM) activities (including Data Flows, Data Models and Governance considerations)?	
Levels	Acceptance Evidence	Acceptance Criteria
	- Model representation.	- Attach a document demonstrating the selection and documentation of a planning method to document business structure, relationships, and code at the conceptual, logical, and physical levels, and use it throughout the software application development life cycle.
	- The DAM Register.	- The entity must attach a Register clarifying the saving mechanism of the following at a minimum: - The Data Architecture & Technical Architecture project. - The reference documentations / materials. - Data Model designs.
	- A document containing the Data Model Representation's Technical Standards & Best Practices.	- The entity must attach a document clarifying that the entity adhered to a standardized method in building Data Models according to best practices (Such as naming conventions, data types, basic attributes, physical model deployment considerations, improvements, etc.).
Level 3: Activated	- The Data Integration Pattern Implementation Document.	- The entity must attach the documents of the Data Integration Pattern diagramming (implemented within the Data Architecture).
	- Evidences of DAM Tools & Technologies in Use.	- The entity must choose & implement a set of technologies to design, develop and execute the entity's DAM initiatives. The set of technological tools shall include, at a minimum: - Data Architecture Design - Visually representing data and system components along with data flow diagramming. - Data Modeling - Drawing functionality to create & modify data and system objects, attributes and relationships, and reverse-engineer the existing data models. - Data Lineage - Capturing and maintaining data flows between systems to enable an impact analysis.
	- Evidences of the Enterprise Data Model Uploaded in the Data Catalog.	- The entity must attach a proof that the Data Catalog has been updated based on new or updated Data Models, to ensure alignment of data models with the Data Catalog.
	- Evidences of Applying the Technical Data Standards.	- The entity must attach (3) samples proving applying Technical Standards on the Data Representation Models, which were pre-defined in the Data Model Representation's Technical Standards Document.
Level 4: Managed	- The Monitoring Report of the Implementation of the DAM Practices with Pre-defined KPIs.	- The entity must attach an updated report, approved by the entity's authority holder, to measure the effectiveness of implementing the DAM plan, based on pre-defined and identified KPIs and indicator cards. - Each indicator card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner.

Checklist – Data Architecture and Modelling Domain

DAM.MQ.2	Has the entity developed and implemented practices for Data Architecture & Modelling (DAM) activities (including Data Flows, Data Models and Governance considerations)?	
Levels	Acceptance Evidence	Acceptance Criteria
		• Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The Continuous Improvement Report Including the DAM Business Procedures Documentation.	- The entity must attach the continuous improvement report for the DAM practices documentation, based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: • Evidence of automation of DAM processes. • Review and results documentation: Periodic review and result documentation for DAM Practices. • Continuous improvement mechanisms: Continuous improvement mechanisms for DAM Practices.

8.2.7.Data Sharing & Interoperability Domain

Checklist – Data Sharing and Interoperability Domain		
DSI.MQ.1	Has the entity developed and implemented a Data Sharing and Integration (DSI) Plan in line with the Data Sharing Policies?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents
Level 1: Establishing	- The Names of the Current Practices of Data Sharing and Integration (DSI).	The entity must attach a list of the names of the current DSI Practices and Activities, including an evidence to support the practice of each Activity, being one of the following, at a minimum: - Email copies / screenshots. - Document Copies. - System screenshots.
	- The Updated and Approved Results of the Initial Data Integration Assessment.	The entity must attach the report of the Data Integration assessment results, including the following, at a minimum: - The current IT Structure: an inventory of all existing IT components (data sources, systems, applications and data stores). - High Level Data Lineage including the rules according to which data is changed, and the frequency of changes. - Data Models used by the entity's IT components. - A list of all identified challenges in data movement and integration path.
Level 2: Defined	- The Developed Data Integration Strategy Document.	The entity must attach the developed Data Integration Strategy containing the following, at a minimum: - The Strategy's approval by the entity's authority holder and effective date. - The Strategy must be recent (Approved within the last three years). - The objectives, initiatives, projects and the metric indicators of the implementation of the Data Integration activities and milestones. The activities shall incorporate what is needed to achieve this Domain's specifications, at a minimum. - The implementation roadmap of the Data Integration initiatives. - The assignment of the required resources & budget allocation to manage the implementation of this Domain.
	- The Developed Target Data Integration Architecture.	The entity must attach the Target Data Integration Architecture including the following, at a minimum: - The Data Integration requirements. - The Data Integration Architecture diagram. - The Architecture components.

Checklist – Data Sharing and Interoperability Domain		
DSI.MQ.1	Has the entity developed and implemented a Data Sharing and Integration (DSI) Plan in line with the Data Sharing Policies?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Developed Data Integration Plan (Including Data Sharing Activities).	The entity must attach a recent and developed Data Integration Plan, approved by the entity's authority holder. including the following, at a minimum: • The summarized Architecture briefs. • The roadmap and covenant charters of the projects and initiatives in the plan. • The assignment of the required resources & budget allocation for the projects and initiatives in the plan.
	- The Developed Data Sharing Policies.	The entity must attach the updated Policies of the Data Sharing & Interoperability (DSI) Domain, approved by the entity's authority holder. The developed policies must align with the updated National Data Governance policies issued by the National Data Management Office (NDMO) - SDAIA. Every Policy document must include, the following, at a minimum: • Policy title / name. • Policy owner. • Release date. • Version number. • Version history. • Objective. • Identified stakeholders (relevant parties). • Communications process. • Monitoring procedure. • Document control (Preparation, review, approval). • Policy Statement. • Roles & responsibilities. • Terminology. • Scope of work. • Activation mechanisms. • Target audience. • Approval. • References.

Checklist – Data Sharing and Interoperability Domain

DSI.MQ.1	Has the entity developed and implemented a Data Sharing and Integration (DSI) Plan in line with the Data Sharing Policies?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Developed Data Sharing Training Plan.	The entity must attach the recent and developed DSI Domain's training and awareness plan, approved by the entity's authority holder, including, the following, at a minimum: • The training and awareness programs plan implementation dates. • The objectives of training and awareness including, at a minimum, the topics stated in the "Data Management and Personal Data Protection (DM & PDP) Standards" document i.e.: • Introduction on the applicability of the Data Sharing process. • The leading / best Data Sharing practices. • The consequences of mishandling data. • The Data Sharing Standards, Controls & Principles. • The methods and channels through which the trainings will be conducted. • Identifying the DSI Domain Awareness campaign channels, which include: • E mails or mobile phone messages. • Publications. • Lectures or workshops.
Level 3: Activated	- A Data Integration Plan Implementation Status Report.	The entity must attach an updated and approved report on the implementation status of the DSI Plan and roadmap, containing the following, at a minimum: • Initiatives and projects status: Identifying the status of each initiative or project (started, in progress, completed, or delayed), along with clarification of any delays or challenges. • Progress percentages: Providing the progress percentages of activities and milestones in the plan and roadmap, with clear details on the actual activities that have been completed. • Supporting evidence: Attaching proof of achieved progress/completion, such as reports, photos, documents, or meeting minutes that support the implementation status.
	- A Report on the Defined Roles and Responsibilities for DSI.	The entity must attach an updated report, approved by the entity's authority holder presenting the DSI Domain's roles and responsibilities including the following, at a minimum: • The stewardship roles of the DSI processes. • The stewardship responsibilities of the DSI processes. • A list of individuals assigned to carry out the roles and responsibilities for the domain.

Checklist – Data Sharing and Interoperability Domain

DSI.MQ.1	Has the entity developed and implemented a Data Sharing and Integration (DSI) Plan in line with the Data Sharing Policies?	
Levels	Acceptance Evidence	Acceptance Criteria
	- A Progress Report on Data Sharing Training Programs.	- The entity must attach an updated report, approved by the entity's authority holder clarifying the DSI training & awareness implementation status containing the following, at a minimum: • The training and awareness target audience. • The list of conducted training programs and awareness campaigns (including the topics of the programs, the dates when they were conducted, the names of the training attendants, and attendance certificates). • Samples of the activities performed by the entity to raise awareness about the DSI Domain, including: • E-mails or mobile phone messages. • Publications. • Lectures or workshops.
Level 4: Managed	- The Monitoring Report with Pre-defined Key Performance Indicators (KPIs) for the Data Integration Plan and Data Sharing Activities.	- The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of the DSI domain implementation plan based on pre-defined and identified KPIs and indicator cards. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values.

Checklist – Data Sharing and Interoperability Domain		
DSI.MQ.1	Has the entity developed and implemented a Data Sharing and Integration (DSI) Plan in line with the Data Sharing Policies?	
Levels	Acceptance Evidence	Acceptance Criteria
		Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	The Continuous Improvement Report on the Data Integration Plan and Data Sharing Activities.	- The entity must attach an updated report, approved by the entity's authority holder presenting the continuous improvements of the DSI Domain's plan based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: - The conducted reviews. - The results of each review. - The implemented enhancements (with supporting documents).

Checklist – Data Sharing and Interoperability Domain		
DSI.MQ.2	Has the entity defined and implemented Processes for Sharing Data within the entity and with other Entities?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents
Level 1: Establishing	Evidences of the Current DSI Practices / Processes by the Entity (Internally & Externally).	The entity must attach a report on the current DSI Practices and Processes, both internally within the entity and externally with other Entities, including an evidence to support the practice of each Activity / Process, being one of the following, at a minimum: - Email copies / screenshots. - Document Copies. - System screenshots.
Level 2: Defined	The Process Documentation for Data Sharing (Including Data Classification Levels and Timelines).	The entity must attach the Data Sharing Process documents with the Process details including the following, at a minimum: - Data Sharing Request Reception. - Identification / assignment of roles. - Data Classification (DC) level check. - Data Sharing Principles assessment. - Data sharing decision and replying with feedback. - Business Data Executive's approval. - Design and implementation of Data Sharing Controls. - Data Sharing Agreement signing. - Sharing Data with the Requestor.
	The Developed and Approved Data Sharing Request Forms (Internal and External).	The entity must attach the Forms of the internal and external Data Sharing requests using the entity's approved templates.
	The Developed and Approved Internal Data Sharing Agreement Template.	The entity must attach the internal Data Sharing Agreements between information systems within the entity.
	The Developed and Approved External Data Sharing Agreement Template.	The entity must attach the external Data Sharing Agreements with other Entities including the following, at a minimum: - The Purpose of Data Sharing. - Information about each requesting and providing entity (that will share their data). - Lawful / Legal / Regulatory basis for Sharing. - Sharing details (Date, Duration, etc.).

Checklist – Data Sharing and Interoperability Domain		
DSI.MQ.2	Has the entity defined and implemented Processes for Sharing Data within the entity and with other Entities?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Liability provisions. - The Data Sharing Agreements signed by the Business Data Executive and the Requestor.
Level 3: Activated	- Evidences of Operationalization of The Data Sharing Process, e.g.: Communication of The Defined Data Sharing Mechanism.	The entity must attach a communication operationalization report related to the defined mechanism of the Data Sharing process, including the following, at a minimum: - Correspondence exchanged proving the establishment of a communication channel between the communicating Entities. - A communication evidence of the approval of a formal mechanism defined for Data Sharing.
	- Evidences of Data Sharing Through SDAIA's Certified and Approved Channels.	The entity must attach a report on the electronic communication with the requestor entity requesting data sharing through the SDAIA-certified and SDAIA-approved channels (e.g.: Data Marketplace (DMP), The Government Service Bus (GSB), etc.). The report may contain: - System screenshots or records. (The communication channel usage can include Data Sharing). - A report on the communications using the entity's formal government website.
	- The Access Authorization Controls Document.	The entity must attach a document detailing the Controls for authorization & usage when accessing the official government website channel for receiving requests.
	- Evidences of Data Sharing Requests Submitted to The Entity and The Requests Submitted by The Entity Through the Established Channel.	The entity must attach the record(s) containing the Data Sharing requests: - The list received by the entity. - The list sent / submitted by the entity.
	- Evidences of the Entity's Responses to the Data Sharing Requests.	The entity must attach the notifications acknowledging receiving the Data Sharing requests with the responses.
	- An Adoption Evidence of The Developed Data Sharing Agreement Template for An Internal Data Sharing Request.	The entity must attach a report containing an evidence of the entity's adoption of a template developed for the Data Sharing Agreement upon an internal request from within the entity.

Checklist – Data Sharing and Interoperability Domain

DSI.MQ.2	Has the entity defined and implemented Processes for Sharing Data within the entity and with other Entities?	
Levels	Acceptance Evidence	Acceptance Criteria
	- An Adoption Evidence of The Developed Data Sharing Agreement Template for An External Data Sharing Request.	The entity must attach a report containing an evidence of the entity's adoption of a template developed for the Data Sharing Agreement upon a request from an external entity.
	- The Documented Review Outcomes of The Data Sharing Agreements.	The entity must attach a report on the results and outcomes of the documented reviews of the Data Sharing Agreements.
Level 4: Managed	- The Monitoring Report with Pre-defined KPIs for the Data Sharing Processes.	The entity must attach an updated report approved by the entity's authority holder on monitoring the effectiveness of the data sharing processes implementation based on pre-defined KPIs (Indicator Cards), covering: • The number of Data Sharing requests received. • The number of Data Sharing requests accepted / denied. • The number of Data Sharing requests sent. • The number of ongoing Data Sharing agreements. • The average duration of the Data Sharing request evaluation process expressed, in days. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value.

Checklist – Data Sharing and Interoperability Domain		
DSI.MQ.2	Has the entity defined and implemented Processes for Sharing Data within the entity and with other Entities?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
	- The Compliance Audit Methodology.	The entity must attach the Compliance Audit Methodology document.
Level 5: Pioneer	- The Continuous Improvement Report on the DSI Processes.	The entity must attach the continuous improvement report of the Data Sharing Processes implementation, based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: - Evidence of DSI Process automation. - The documents of the periodic reviews, evaluations & documented results of the DSI Domain Processes. - Improvements implemented (with supporting documents).

Checklist – Data Sharing and Interoperability Domain		
DSI.MQ.3	Has the entity defined and implemented a data integration architecture to manage the data movement efficiently across data stores, systems, and applications?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents
Level 1: Establishing	- Evidences of Data Movement / Integration within the Entity and with Other Entities.	The entity must attach evidences of Data Movement or Data Integration / Interoperability: - Internally within the entity. - Externally with other entities.

Checklist – Data Sharing and Interoperability Domain

DSI.MQ.3	Has the entity defined and implemented a data integration architecture to manage the data movement efficiently across data stores, systems, and applications?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 2: Defined	- The Integration Requirements Document.	The entity must attach the Integration / Interoperability Requirements document containing the following, at a minimum: • A clearly defined scope. • Entity's Business goals / objectives and aims to be achieved. • Implementation Timeline. • Resources required. • Cost estimate. • Functional requirements. • Non-Functional requirements.
	- The Solution Design Document.	The entity must attach the Solution Design document including the following, at a minimum: • Integration Solution Overview. • Target Data Integration Architecture. • Data Orchestration – The Data Flow Diagram (DFD). • Source to Target Mapping – A set of Data Transformation instructions that determine how to convert the structure and content of data in the source system to the structure and content needed in the target system. The instructions shall include the following, at a minimum: • The technical format of data at the source and the target. • The Specifications of transformations required for all intermediate-staging points between the source and the target.
Level 3: Activated	- The Document of the Approved Standardized Entity Wide Integration Solution Development Lifecycle.	The entity must attach a life cycle description document, being the standardized and approved cycle for the development of Integration/Interoperability solutions at the entity level. The description should include the stages of the lifecycle for developing Integration/Interoperability solutions, roles and responsibilities, as well as practices implemented during the lifecycle of solution development.
	- The Developed Test Scripts and the Conducted Tests (Integration, Functional) in Line with the Plan and the Solution Design Document.	The entity must attach the developed test scripts and the conducted tests (Integration tests & functional tests) in alignment with the Plan and the Solution Design document, containing the following, at a minimum: • The defined & identified Test Use Cases. • Evidence of a Test Environment setup. • The Test Use Cases executed in a Test Environment and the documented test results.

Checklist – Data Sharing and Interoperability Domain

DSI.MQ.3	Has the entity defined and implemented a data integration architecture to manage the data movement efficiently across data stores, systems, and applications?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 4: Managed	- The Monitoring Report with Pre-defined KPIs for the Data Integration Initiatives.	The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of implementing data Integration / Interoperability initiatives based on the data of the KPIs (Indicator Cards) which were pre-defined for the DSI Domain, covering: • Data transfer rate between systems/applications. • Latency between data sources and data targets. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values
	- The Integration Solution Monitoring and Maintenance Document.	The entity must attach a document on monitoring and maintaining the Integration / Interoperability solutions, containing the following, at a minimum: • Reports of any detected programming flaws or errors. • Change requests from end users to incorporate changes in business requirements.

Checklist – Data Sharing and Interoperability Domain		
DSI.MQ.3	Has the entity defined and implemented a data integration architecture to manage the data movement efficiently across data stores, systems, and applications?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 5: Pioneer	- The Continuous Improvement Report on the Data Integration Practices.	The entity must attach an updated & approved report to improve the implementation of data Integration/Interoperability initiatives, based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum - The documents of the periodic reviews & documented results. - Improvements implemented (with supporting documents).
	- The Continuous Improvement Mechanisms for Data Integration, e.g.: Continuous Integration & Continuous Delivery (CICD) Pipeline Details for Automation.	The entity must attach a document clarifying the details of the automation activities program (Pipeline) in relation to Continuous Integration & Continuous Delivery (CICD).

Checklist – Data Sharing and Interoperability Domain		
DSI.MQ.4	Has the entity developed and implemented Data Sharing Controls and Processes for efficient Data transformation and movement?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents
Level 1: Establishing	- The Existing Data Integration or Data Movement Processes within the Entity.	The entity must attach a report on the current Data Integration / Interoperability Processes or the current Data Movement Processes within the entity.
Level 2: Defined	- The Developed Data Migration Processes (i.e.: ETL).	The entity must attach a report on the Processes and Standards process to integrate data from disparate sources and load it into the Data Warehouse Store i.e.: Extract, Transform, Load (ETL).
	- The Developed Data Migration Processes (i.e.: ELT).	The entity must attach a report on the Processes and Standards process to store the unstructured data in its raw native format in the Data Lake i.e.: Extract, Load, Transform (ELT).

Checklist – Data Sharing and Interoperability Domain

DSI.MQ.4	Has the entity developed and implemented Data Sharing Controls and Processes for efficient Data transformation and movement?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Risk Assessment Report on the Entity's Datasets to be Shared.	The entity must attach an assessment report on the risks which may arise as a result of sharing the entity's datasets.
	- The Defined Data Sharing Controls.	The entity must attach a report on the Controls that have been identified and defined for Data Sharing.
Level 3: Activated	- Evidence of the Implemented Data Migration Processes (i.e.: "Extract, Transform, Load (ETL)).	The entity must submit a report to showcase the Implemented "Extract, Transform, Load (ETL)" process for integrating data from disparate sources and loading into Data Warehouse Store. The process must include the following steps: • Extract – Data Extraction must include the following, at a minimum: • Identification of Data Sources from which the data will be extracted. • Extracting data from the Data Sources. • Staging the extracted data temporarily in a physical data store, e.g.: On disk or in another memory. • Transform – The Data Transformation step must include the following, at a minimum: • Data Mapping – Planning the actual transformation process. • Data Transformation – Removing duplicate data, filling out missing values, filtering, sorting, joining and splitting data. • Review – Validating the correctness of the transformation. • Load – Physically storing the transformed data in the Data Warehouse / Store.
	- Evidence of the Implemented Data Migration Processes (i.e.: "Extract, Load, Transform (ELT)).	- The entity must submit a report to showcase the Implemented "Extract, Load, Transform (ELT)" process for storing unstructured data in its raw native format in the Data Lake. The process must include the following steps: • Extract – The Data Extraction step must include the following, at a minimum: • Identification of Data Sources from which the Data will be extracted. • Extracting data from Data Sources.

Checklist – Data Sharing and Interoperability Domain

DSI.MQ.4	Has the entity developed and implemented Data Sharing Controls and Processes for efficient Data transformation and movement?	
Levels	Acceptance Evidence	Acceptance Criteria
	- A Report on the Implemented Controls (e.g.: Data Security & Protection, Data Sharing, Data Integration, Data Access, etc.).	• Loading – Physically storing data in its raw native format in the Data Lake. • Transform – The Data Transformation step must include the following, at a minimum: • Data Mapping – Planning the actual transformation process. • Data Transformation – Removing duplicate data, filling out missing values, filtering, sorting, joining and splitting data. • Review – Validating the correctness of the transformation. - The entity must attach a report clarifying the Controls implemented on the Migration Processes “ETL or ELT” (e.g., Controls for: Data Sharing, Data Integration / Interoperability, and Data Access Authorizations, etc.), including the following, at a minimum: • Attaching an evidence that all stakeholders involved in Data Sharing applied the appropriate Security Controls to protect and share data, in a safe and reliable environment, in alignment with the relevant laws and regulations, and as issued by the National Cybersecurity Authority (NCA). • Attaching an evidence that all stakeholders involved in Data Sharing have the following, at a minimum: • The authorization to view, obtain / acquire and use this data (which may require security scanning depending on the nature and sensitivity of the data based on the Data Classification (DC) Domain Standards). • Knowledge, skill, and qualified people who are properly trained on handling the Shared Data. • Attaching an evidence that all stakeholders involved in Data Sharing applied the controls which are necessary to appropriately manage and protect the Shared Data, including what is stated in the National Data Governance (DG) Policies issued by SDAIA, e.g.: • Legal / Regulatory basis. • Delegation / Authorization. • Data type. • Data pre-processing. • Data Sharing methods. • Data usage & maintenance. • Data Sharing duration. • The number of times data was Shared. • Sharing cancellation. • Liability provisions.

Checklist – Data Sharing and Interoperability Domain

DSI.MQ.4	Has the entity developed and implemented Data Sharing Controls and Processes for efficient Data transformation and movement?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 4: Managed	- The Monitoring Report with Pre-defined KPIs for the DSI Controls, Processes and Standards.	The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of DSI Controls, Practices and Standards implementation based on pre-defined and identified KPIs and indicator cards, and each indicator's data or card should include the following, at a minimum: - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The Continuous Improvement Report on Reviewing the DSI Processes and Mechanisms to Automate the DSI Controls and Practices.	The entity must attach an updated and approved report on the continuous improvement of processes and mechanisms implemented to automate the DSI Domain's Controls, Standards, and Practices, including the following, at a minimum: • The documents of the periodic reviews & documented results. • Improvements implemented (with supporting documents).

8.2.8. Reference and Master Management Data Domain

Checklist – Reference and Master Data Management Domain		
RMD.MQ.1	Has the entity developed and implemented a plan focused on improving its Reference & Master Data (RMD) Management capabilities?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents
Level 1: Establishing	- The Currently Existing Practices Related to the RMD Management and Planning Domain.	A report must be attached clarifying the current practices related to Reference Data management and/or Master Data management.
Level 2: Defined	- The Developed and Approved RMD Management Plan.	A recent RMD Management Plan, approved by the entity's authority holder must be attached including the following, at a minimum: - A roadmap that includes the activities and milestones for the entity's RMD Management. The activities shall incorporate what is needed to achieve this Domain's specifications, at a minimum. - The assignment of the required resources & budget allocation to manage the implementation of the roadmap activities.
Level 3: Activated	- The RMD Management Plan Implementation Status Report.	A report must be attached clarifying the implementation status and roadmap of the RMD Management Plan including the following, at a minimum: Initiatives and projects status: Identifying the status of each initiative or project (started, in progress, completed, or delayed), along with clarification of any delays or challenges. Progress percentages: Providing the progress percentages of activities and milestones in the plan and roadmap, with clear details on the actual activities that have been completed. Supporting evidence: Attaching proof of achieved progress/completion, such as reports, photos, documents, or meeting minutes that support the implementation status.
	- The RMD Management Training Implementation Status Report.	A report must be attached clarifying the implementation status including the following, at a minimum: - Attach samples of the activities performed by the entity to raise awareness in the RMD Management Domain (Awareness messages, publications, lectures or workshops). - Attach a sample attendance certificate of training the entity's employees in the RMD Management Domain.
	- The RMD Management Operating Model Showing the RMD Stewardship Coverage.	A document must be attached confirming that the entity has designated Business Data Stewards and IT Data Stewards to manage each defined set of RMD.

Checklist – Reference and Master Data Management Domain		
RMD.MQ.1	Has the entity developed and implemented a plan focused on improving its Reference & Master Data (RMD) Management capabilities?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The RMD Change Request Logs.	A consolidated log must be attached containing the following, at a minimum: - The RMD change requests. - The decisions made on the RMD change requests.
	- The RMD Management Documents & Artifacts.	The planning documents & supporting artifacts of the RMD Management initiatives must be attached including the following, at a minimum: The register of the Architecture status of all RMD initiatives (e.g., The Statement of Architecture Work (Scope) document).
Level 4: Managed	- The Monitoring Report of the RMD Management Plan Implementation with Pre-defined KPIs.	- The entity must attach an updated report, approved by the entity's authority holder, on monitoring the effectiveness of implementing the RMD Management Plan based on pre-defined and identified KPIs and indicator cards. - Each indicator card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values

Checklist – Reference and Master Data Management Domain		
RMD.MQ.1	Has the entity developed and implemented a plan focused on improving its Reference & Master Data (RMD) Management capabilities?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 5: Pioneer	- The Continuous Improvement Report of the RMD Management Plan.	- The entity must attach an updated report, approved by the entity's authority holder presenting continuous improvement of the RMD Management Plan based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: • Reviews conducted. • Results of each review. • Improvements implemented (with supporting documents).

Checklist – Reference and Master Data Management Domain		
RMD.MQ.2	Has the entity defined and implemented processes to manage its Reference & Master Data (RMD) objects from creation to archival?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents
Level 1: Establishing	- Evidence of Projects / Initiatives with Reference Data and/or Master Data Identified.	An evidence must be attached proving the implementation of any existing project or current initiative that involves identified Reference Data and/or Master Data Objects.
Level 2: Defined	- The Identified, Prioritized and Categorized RMD Objects.	Documents must be attached clarifying that the entity identified, prioritized & categorized the RMD including the following, at a minimum: - Identifying & Prioritizing the RMD: - The identified Master Data objects (internal & external). - The identified Reference Data objects (internal & external). - The identified data sources and applications that generate, read, update, and delete RMD Objects. - The logically grouped & prioritized RMD Objects.
	- Reference Data Categorization.	Attach documents showing that the entity has categorized the reference data. These documents include, at a minimum, the following: - Internal Reference Data. - External Reference Data.
	- Master Data Categorization.	Attach documents showing that the entity has categorized the reference data. These documents include, at a minimum, the following: - Internal Master Data. - External Master Data.
	- The Reference & Master Data Requirements.	Evidence documents must be attached clarifying that the entity collected the RMD requirements including the following, at a minimum: - RMD Management roles across the data lifecycle from creation to archiving. - Rules for accurate matching and merging of the Master Data Records from different data sources to create Golden Records. - Requirements for provisioning Master Data Golden Records to consuming applications. - Requirements for provisioning Reference Data Objects to consuming applications. - Data Quality (DQ) requirements for RMD Objects to be leveraged as input for the Initial Data Quality Assessment detailed in the Data Quality (DQ) Domain.

Checklist – Reference and Master Data Management Domain		
RMD.MQ.2	Has the entity defined and implemented processes to manage its Reference & Master Data (RMD) objects from creation to archival?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Defined SLAs for RMD Lifecycle Management.	- A document should be attached clarifying the RMD lifecycle management process SLAs including, at a minimum: • The RMD request implementation time frame. • The escalation procedures to be done upon SLA violation.
Level 3: Activated	- The RMD Lifecycle Management Process.	- A document must be attached clarifying a process for managing RMD Objects across the Data Lifecycle from creation to archival / disposal. The process must cover roles and procedural actions involved in the following Data Lifecycle steps, at a minimum: • Creating new RMD Objects & Instances. • Modifying existing RMD Objects & Instances. • Archiving RMD Objects & Instances.
	- Evidence of the Entity's Participation in or Use of National Reference Datasets.	- The entity must attach a sample of evidence demonstrating its participation in or utilization of the National Reference Datasets. The samples must include the following at a minimum: • A screenshot of the entity's reference datasets shared on the National Reference Data Platform. • A screenshot of the reference datasets utilized by the entity through the National Reference Data Platform. • A screenshot demonstrating the processes conducted to upload the entity's reference data to the National Reference Data Platform.
Level 4: Managed	- The Monitoring Report of the RMD Management Processes with Pre-defined KPIs & SLAs.	- The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of the RMD Management Processes, based on pre-defined and identified KPIs and indicator cards, covering the following: • The number of incorrect data values in the Master Data Records. • The Mean Time to Repair (MTTR) RMD quality issues. • The volume of change requests submitted to modify RMD Objects. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline.

Checklist – Reference and Master Data Management Domain		
RMD.MQ.2	Has the entity defined and implemented processes to manage its Reference & Master Data (RMD) objects from creation to archival?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The Continuous Improvement Report of the RMD Management Processes & Standards.	- The entity must attach the continuous improvement report of the RMD Management Processes, based on the results of the KPI measurements and relevant updates and developments in the domain, containing the following, at a minimum: - Evidence of the RMD Management Processes automation. - Review and results documentation: Periodic review and result documentation of the RMD Management Processes. - Continuous improvement mechanisms: Continuous improvement mechanisms of the RMD Management Processes.

Checklist – Reference and Master Data Domain		
RMD.MQ.3	Has the entity implemented a Data Hub (or Tool) as the trusted Data source to support the RMD Management Processes?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents
Level 1: Establishing	- Evidence That the Entity Manages Its RMD Within	The entity must provide proof of managing reference and/or master data within databases used for the purposes of an ongoing specific project.

Checklist – Reference and Master Data Domain		
RMD.MQ.3	Has the entity implemented a Data Hub (or Tool) as the trusted Data source to support the RMD Management Processes?	
Levels	Acceptance Evidence	Acceptance Criteria
	Independent Data Sources and Without Unified Tools.	
Level 2: Defined	- The Target RMD Management Architecture Design.	A document must be attached illustrating that the entity designed an RMD Hub to efficiently manage the RMD Objects including, at a minimum: - Identifying a Data Hub architecture implementation pattern to manage the Master Data Objects, based on its specific RMD requirements. - The design considers supporting centralized management of Reference Data. The Hub is the single source of Reference Data, with creation and modification operations performed exclusively within the Hub. All critical consumer applications must use the Hub as the reference data source.
	- The Developed RMD Conceptual Architecture.	The target RMD environment Conceptual Architecture must be attached as per the entity's selected Data Hub architecture design; indicating foundational building block components and high-level capabilities associated with the components. The conceptual RMD architecture must consist of the following, at a minimum: - Architecture Description – A description of the overall architecture concept defined. - Components Definitions and Descriptions – Building blocks (The Data Hub, data sources, consuming applications, etc.) of the RMD Conceptual Architecture with descriptions of their purposes. - The General Conceptual Architecture Diagram – A high-level view of how components work together to address the entity's RMD requirements.
	- The Developed RMD Information Architecture.	A document must be attached clarifying an Information Architecture for the target RMD environment based on the defined Conceptual Architecture. The Information Architecture must represent the following components, at a minimum: - RMD Objects – An inventory of the identified RMD Objects including Metadata definitions. - Conceptual & Logical Master Data Model – A conceptual & logical Data model for the identified Master Data Objects and their relationships. - RMD Sources – An inventory of the identified RMD sources. - Rules for Matching & Merging Master Data Records from different data sources to create Golden Records. - RMD Flows - One-way or two-way movement for: - Master data records between data sources and the data hub. - Golden records of master data between the data hub and critical consuming applications.

Checklist – Reference and Master Data Domain

RMD.MQ.3	Has the entity implemented a Data Hub (or Tool) as the trusted Data source to support the RMD Management Processes?	
Levels	Acceptance Evidence	Acceptance Criteria
		Reference data between the data hub and critical consuming applications.
	- The RMD Hub / Tool Technical Requirements.	A document must be attached defining, identifying & documenting the technical requirements for the RMD Hub platform based on the defined target RMD Information Architecture. The requirements must cover the following areas, at a minimum: - Management of Workflows: - Creating & modifying RMD Records. - Assigning Master Data Management (MDM) Stewardship. - Versioning Control - Tracking changes in RMD Records over time. - Functional Capabilities – Detailing the functional capabilities required from the Hub (e.g.: Import, export, data mappings, automation of operational tasks around collection, cleansing, etc.). - Technical Capabilities - Detailing the technical capabilities required from the Hub (e.g., API Integration with upstream & downstream applications and systems). - Security - Supporting secure data exchange between the Hub and the connected applications / data sources.
Level 3: Activated	- The Implemented RMD Management Hub.	- A document must be attached providing evidence that the entity implemented an integrated Hub for managing its RMD Objects to be considered as the entity's trusted source of RMD. The document must provide evidences for the following performed tasks, at a minimum: - The instantiated physical Data Hub Technical Architecture components necessary to address the entity's target RMD Information Architecture requirements. - The established Master Data Model as defined by the RMD Information Architecture within the Data Hub. - The loaded RMD Objects into the Data Hub. - The necessary replication activated between Master Data Source systems and the Data Hub. - Synchronization activated between the Data Hub and the consuming applications.
	- The Workflow Documentation Showing the Establishment of the Data Hub as the Entity's Trusted Source.	- An evidence must be attached proving that the Data Hub is considered a reliable source for each information system or new application that requires the use of special RMD Objects (for each program).

Checklist – Reference and Master Data Domain

RMD.MQ.3	Has the entity implemented a Data Hub (or Tool) as the trusted Data source to support the RMD Management Processes?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 4: Managed	- The Monitoring Report of the RMD Management Hub / Tool Capabilities with Pre-defined Key Performance Indicators (KPIs).	- The entity must attach an updated report, approved by the entity's authority holder, to monitor the RMD Management Hub/Tool capabilities, based on pre-defined and identified KPIs and indicator cards. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The Continuous Improvement Report of the RMD Information Architecture and the Implemented Data Hub.	- The entity must provide the continuous improvement report for the RMD Management Hub/Tool, based on the results of the KPI measurements and relevant updates and developments in the domain, containing the following, at a minimum: • Review and results documentation: Periodic review and result documentation for the RMD Hub/Tool performance. • Continuous improvement mechanisms: Continuous improvement mechanisms for the RMD Hub/Tool.

8.2.9. Business Intelligence and Analytics Domain

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.1	Has the entity developed and implemented a plan to manage and orchestrate its Business Intelligence & Analytics (BIA) activities?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- Current activities related to BIA.	- A document must be attached, covering: Current activities related to BIA (reports and/or dashboards, etc.).
Level 2: Defined	- The defined & approved BIA Plan.	- A recent BIA plan, approved by the entity's authority holder must be attached, and the plan must include the following, at a minimum: - A roadmap of activities and milestones for Data Analytics & Artificial Intelligence (DA & AI) use cases. The activities should include what is necessary to achieve this Domain's specifications, at a minimum. - The allocation of the required resources & budget to manage the implementation of the DA & AI use cases.
Level 3: Activated	- The BIA plan & roadmap implementation status report.	- A status report of the BIA Plan & roadmap implementation must be attached, which includes at a minimum: Initiatives and projects status: Identifying the status of each initiative or project (started, in progress, completed, or delayed), along with clarification of any delays or challenges. Progress percentages: Providing the progress percentages of activities and milestones in the plan and roadmap, with clear details on the actual activities that have been completed. Supporting evidence: Attaching proof of achieved progress/completion, such as reports, photos, documents, or meeting minutes that support the implementation status.
	- The Defined & Documented Roles & Responsibilities for BIA Activities Including Data Stewardship Roles.	- A document must be attached showing the roles & responsibilities of the data team members working on the BIA Activities' Implementation including, at a minimum: The defined & documented roles & authorizations of all data specialists, including the Data Stewards & Data Owners.
Level 4: Managed	- The Effectiveness Monitoring Report of the BIA Plan & Activities According to the Pre-Defined Key Performance Indicators (KPIs).	- The entity must attach an updated report, approved by the entity's authority holder, on monitoring the effectiveness of the BIA Plan & Activities' based on pre-defined and identified KPIs and indicator cards. - Each indicator card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator.

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.1	Has the entity developed and implemented a plan to manage and orchestrate its Business Intelligence & Analytics (BIA) activities?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- Regular reviews and improvements to the business intelligence and analytics plan and roadmap.	- The entity must attach an updated report, approved by the entity's authority holder presenting continuous improvement of the BIA Plan domain, based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: - Reviews conducted. - Results of each review. - Improvements implemented (with supporting documents).

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.2	Has the entity identified BIA use cases and defined a plan for the use case implementation?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents.	- No required documents

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.2	Has the entity identified BIA use cases and defined a plan for the use case implementation?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 1: Establishing	List of the implemented BIA uses cases within the Entity.	- The document must include a list of the use cases implemented within the entity, and for each use case included in the specified list, the following must be documented, at a minimum: - The name of the use case. - The description of the use case. - The desired & the achieved objectives of the use case.
Level 2: Defined	The approved BIA business cases / BIA use cases.	- A document containing the following, at a minimum, must be attached: - The list of approved BIA Business Cases: Business cases define the strategic reasons, logical justifications, expected benefits, and ROI resulting from implementing BIA projects. - The list of approved BIA use cases: Use cases represent the practical and functional needs related to analyzing and utilizing data within the entity. - For each business case / use case in the identified lists, the following must be documented, at a minimum: - The name of the case. - The description of the case. - The stakeholders of the case. - The list of business cases and use cases for BIA must be approved by the entity's authority holder and remain valid.
	The approved BIA Use Cases Prioritization Framework.	- A document must be attached that includes the approved framework for shortlisting / prioritizing BIA use cases, and the document must include the following, at a minimum: - Prioritization Identification Criteria: A list of criteria used to prioritize use cases such as strategic alignment, potential impact, complexity, and resource requirements. - Weighting Criteria: An explanation of how each criterion is weighted and how weighting is specified. This can be based on opinions of experts, inputs from stakeholders, a data-driven approach, etc. - Scoring Mechanism: A description of how scores are calculated to weight & specify use case priorities. The framework must be approved by the entity's authority holder and remain valid.

Checklist – Business Intelligence and Analytics Domain

BIA.MQ.2	Has the entity identified BIA use cases and defined a plan for the use case implementation?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The shortlisted / prioritized use cases based on business needs.	- A document must be attached, listing the high-priority use cases based on the pre-approved prioritization framework. For each use case in the prioritization list, the following must be documented, at a minimum: • The name of the use case. • The description of the case. • The priority of the case. - Note, if there is a single document containing the approved use cases, and / or approved framework, and/or prioritized use cases, this evidence can be attached to this requirement and the previous two requirements.
	- The BIA Use Case Portfolio document with details of each use case.	- A portfolio document of BIA use cases must be attached, and the following details must be documented for each use case, at a minimum: • The desired & achieved objectives of each use case. • Type of Analytics leveraged (among the five Analysis-Maturity levels, which are Discovery, Descriptive, Diagnostic, Predictive, Prescriptive). • The expected benefits & business value aimed to be derived (Return on Investment (ROI) through the development of each business case. • Stakeholders & Entities involved in the implementation of the use case, the responsible 'owner' who'd lead the use case, and the target consumers who'd benefit from the insights generated by the use case. • A list of business requirements needed to implement the use case. • Data sources that would feed the use case, with the required data fields. • The technologies required to implement the use cases. • Case priority.
	- The Approved Use Case implementation plan.	- An approved BIA use case implementation plan must be attached including: • The implementation plan for each shortlisted / prioritized & approved Use Case, with the succession order of the implementation steps from the use case trial / piloting phase, getting through the production phase toward continuous result monitoring. The implementation plan shall address the following, at a minimum: • To detail Functional & Non-Functional Requirements – Use case objectives translated into analytics requirements. • High Level Design – Conceptual design of the analytics solution, (e.g., Wireframes). • Staging & Production Environment Preparations – Analytics solution hosting environments during and after development.

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.2	Has the entity identified BIA use cases and defined a plan for the use case implementation?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Development – Functional & non-functional requirements to be developed to meet the high-level design. - Testing – Scopes & types of testing that must be conducted. - Deployment & Schedule – Timeline for establishing a pilot and / or delivery of the complete use case. - Required Resources – The entity's key personnel who have the needed skills, expertise & knowledge to successfully implement the Data Analytics Use Case. - Acceptance Criteria – Key criteria for measuring the successful implementation of the Data Analytics use case. The plan must be approved by the entity's authority holder and remain valid.
	- The defined use case implementation approach (e.g. DevOps, Agile, etc.).	- A use case implementation methodology document must be attached, representing the systematic and organized process followed for implementing each use case. The document must include the following, at a minimum: - The methodology general description. - Key practices & tools in the approach. - The roles & responsibilities of the participants in the approach.
	- The approved use case validation process.	- A validation process document must be attached showing how to validate use case outcomes, stating the initial intended purpose, and explaining the alignment with the entity's overall Data Analytics Plan. The validation of use cases shall address the following, at a minimum: - Analytics Use Case functional and non-functional requirements. - Analytics Use Case Personal Data Protection (PDP) considerations, as prescribed in the Privacy / PDP Domain. - Data Analytics Use Case Return on Investment (ROI) for each target set. The validation process must be approved by the entity's authority holder and remain valid.
Level 3: Activated	- The Implemented and new Use Cases.	- A document must be provided that includes a list of implemented use cases, as well as another list of new use cases that have been evaluated and implemented according to business requirements. For each use case in the specified list, the following must be documented, at a minimum: - The name of the use case. - The description of the case. - The priority of the case.
	- The up-to-date BIA use cases register.	- An up-to-date register of use cases must be attached showing the following, at a minimum: - The Register's Releases (with the dates). - BIA use cases.

Checklist – Business Intelligence and Analytics Domain

BIA.MQ.2	Has the entity identified BIA use cases and defined a plan for the use case implementation?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Outcomes of the BIA Use Case Validation Processes.	• The Results of the final reviews of each use case implementation. • The stakeholders in the entity who can view the register. - A document must be attached showing the outcomes of the BIA use case validation activities, and it must include the outcome of each use case validation process, stating the initial intended purpose, and explaining the alignment with the entity's overall Data Analytics Plan. The use case validation outcomes document must include the following, at a minimum: • Analytics Use Case functional and non-functional requirements. • Analytics Use Case Personal Data Protection (PDP) considerations, as prescribed in the Privacy / PDP Domain. • Data Analytics Use Case Return on Investment (ROI) for each target set.
Level 4: Managed	- The Monitoring Report on the BIA Portfolio Effectiveness with pre-defined Key Performance Indicators (KPIs).	- The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of the BIA portfolio based on pre-defined and identified KPIs and indicator cards, containing the following, at a minimum: • The number of the identified / shortlisted use cases. • The number of use cases in the pilot / beta phase for testing. • The number of the implemented use cases that are widely utilized. • The total Return on Investment (ROI) value generated from use case implementations. • Other potential Key Performance Indicators (KPIs) include (but are not limited to): • Accuracy in achieving desired outcomes from analytical models. • Number of positive impacts resulting from implementing use cases on business aspects, such as process improvement or enhancing user experience. • Number of positive impacts resulting from implementing use cases on technical aspects, such as increased adherence to technical standards. • Number of positive impacts resulting from implementing use cases on strategic decisions. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation.

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.2	Has the entity identified BIA use cases and defined a plan for the use case implementation?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The continuous Improvement Report on BIA Use Cases.	- An updated report must be attached on the Continuous Improvement of the BIA Use Cases, based on the results of the KPI measurements and relevant updates and developments in the domain including the following for each use case, at a minimum: - Potential impact. - The process and innovation methods used to improve the use case, along with an explanation of the outcomes of the process and methods applied to enhance it. - Competitive Advantage. - Total Cost of Ownership (TCO) Analysis: - Analyzing all expenses over the life of the project or per task. - The description of the updated TCO calculation methodology, with any assumptions or estimations applied during the calculation. - Return on Investment (ROI) Analysis: - Analyze all benefits achieved such as revenue increases, cost savings, or productivity gains, in comparison with the expenses per project or per task. - The description of the updated ROI calculation methodology, with any assumptions or estimations applied during the calculation.

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.2	Has the entity identified BIA use cases and defined a plan for the use case implementation?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Updated BIA Use Case Register and the Optimized Use Cases.	- An updated use case record must be attached including the following, at a minimum: • The Revised & improved use cases.

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.3	Has the entity defined and implemented practices to manage and govern the BIA processes?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- The Existing BIA Domain Processes & Governance Documentation.	- A document must be attached covering the following, at a minimum: • The details of the current BIA Processes. • The current BIA Governance documents.
	- The List of Existing Reports & Dashboards.	- A document must be attached covering the following, at a minimum: • The current Reports. • The current Dashboards.
Level 2: Defined	- The Developed & Approved Processes of BIA Management.	- A document containing details of the developed and approved processes for managing business intelligence and analytics should be attached, which should include, at a minimum, the following: • Data warehouse or Data Lake processes with logical models for modeling business functions. The processes must be approved by the entity's authority holder and remain valid.
	- The Approved Process of New Data Source Requirements.	- A document must be attached containing the approved process management procedures of identifying, evaluating, and approving new sources of data to be used in BIA applications. The document must include, at a minimum: • Data Source Identification: This includes identifying new sources which may have processes that are related to the entity's BIA needs, e.g., External data sources or internal data sources from units within the entity. • Data Source Evaluation: This involves evaluating new sources which are proposed based on factors such as Data Quality (DQ), alignment with the business objectives, and cost-benefit considerations.

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.3	Has the entity defined and implemented practices to manage and govern the BIA processes?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Prioritizing Data Sources: This includes giving priority to proposed new sources based on the importance of their data and their impact on the entity's BIA activities. - Data Source Approval / Agreement: This includes obtaining the necessary stakeholder approvals, e.g., Data Owners, IT Teams & Business Leaders.
	- The Approved Demand Management Process.	- The approved process document of BIA Demand Management must be attached showing the following: - Demand Analysis: The process of analyzing the BIA service demand, including request volume, frequency, and complexity. - Request Prioritization: The process of prioritizing BIA service requests, including the criteria that will be used to prioritize each request. - Resource Allocation: The process of allocating resources to support the BIA service demand. - Communication: The process of communicating the BIA service demand status to the stakeholders, and about the performance of the Demand Management process. - Governance & Compliance: The Governance & Compliance process to implement this approved process for BIA service Demand Management. The processes must be approved by the entity's authority holder and remain valid.
	- Development and maintenance document of the Semantic Layer.	- The document for the development and maintenance of the semantic layer in the business intelligence and analytics solution should be attached. It acts as a bridge between data sources and end users by providing a logical representation of the data to facilitate understanding and usage. The document should include, at a minimum, the following: - Data Source Mapping: The mapping between Data Sources and the Semantic Layer, i.e., How the data from each source is mapped on to the Semantic Layer, including any transformations or collations performed. - Business Logic: The Business Logic is applied to the data in the Semantic Layer. This shall include entity-specific definitions of key business concepts. - Security: This section describes how security is implemented in the Semantic Layer. It shall define the security roles & permissions that apply to the data. - Performance Optimization: The strategies used to enhance the Semantic Layer's performance. The strategies shall include technologies such as

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.3	Has the entity defined and implemented practices to manage and govern the BIA processes?	
Levels	Acceptance Evidence	Acceptance Criteria
		indexing / cataloging, caching / temporary storage, and clustering to improve query performance. - Metadata: The Metadata associated with the Semantic Layer, including data descriptions, and definitions of business concepts. - User Interface: The components of the User Interface used to access and interact with the Semantic Layer, e.g., Dashboards, reports, and data discovery / exploration tools. - Record and results of any maintenance performed on the semantic layer.
	Advanced analytics management and governance process.	- The document for the management and governance of advanced analytics should be attached. The document must include, at a minimum: - The Advanced Analytics Governance Framework. - The operations & the procedures of Data Management in the Advanced Analytics context. - The operations & the procedures of the Development Management of the Models used in Advanced Analytics, deployment, and maintenance. - The security & compliance procedures in the context of advanced analytics. - The operational procedures of advanced analytics. - The continuous improvement operations & procedures of advanced analytics. This shall include procedures for measuring the Advanced Analytics effectiveness to identify improvement areas and implement the modifications. The process must be approved by the entity's authority holder and remain valid.
	The Developed & Approved Change Management Plan including the training programs.	- The developed & approved Change Management Plan (for training programs) must be attached including the following, at a minimum: - The details of BIA training to be conducted for all employees participating in BIA initiatives to raise the level of analytical capabilities within the entity. The training shall include the following, at a minimum: - Methods of collecting & organizing the data required for the analysis. - Model Development, Analysis Method Implementation, and Analytical Tool Usage. - The Development of Data Models and Data Flow Paths. - The Types of Graphic Representations of Data & Information. - The Analysis Models Evaluation Methods. The process must be approved by the entity's authority holder and remain valid.

Checklist – Business Intelligence and Analytics Domain

BIA.MQ.3	Has the entity defined and implemented practices to manage and govern the BIA processes?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Developed & Approved Change Management Plan including awareness campaigns.	- The developed & approved Change Management Plan (for Awareness Campaigns) must be attached including the following, at a minimum: • The details of the BIA Domain's awareness campaigns to enhance familiarity, knowledge & usage of the Data Analysis (DA) & Artificial Intelligence (AI) capabilities. The entity shall use one or more of the communication channels (owned by the entity) for awareness campaigns to raise edification of the following: • The Analytics Assets that the entity currently owns – previously implemented use cases, analysis models, Application Programming Interfaces (APIs), BI reports, and the monitoring dashboards utilized; all of the above for probable data sharing and potential reuse. • BIA Success Stories – Quantitative & qualitative benefits and outcomes from recent use case implementation activities. • The new tools used in the BIA Domain and the technical tool workflows in the entity Especially those tools that are based on emerging new technologies. The plan must be approved by the entity's authority holder and remain valid.
	- The identified & developed Data Sources & Data Marts.	- A document should be attached that includes, at a minimum, the following: • Data Sources: e.g., Systems, databases, or applications that create, store, or manage data that will be used in BIA. They can include Internal Data Sources, such as transactional databases, data storages, and data lakes; in addition to External Data Sources, such as social media communication methods, market research reports, and publicly available datasets. • Data Marts: Subsets / partitions of data warehouses designed to serve particular business units or specific job functions.
Level 3: Activated	- Evidences of the adoption & implementation for business intelligence and analytics management and governance.	- A document must be attached including the following: • Proofs of adopting and implementing all business intelligence and analytics management and governance processes. • Proofs of adopting and implementing comprehensive governance that includes emerging topics such as ethics of artificial intelligence. • Proofs of adopting and implementing advanced analytics management and governance processes (AI/ML Ops).
	- The approved Operating Model with defined roles & responsibilities for The Data Science team.	- A document must be attached showing the following: • The approved Operating Model of the Data Science team. • Process flow documentation. • The roles & responsibilities of the Data Science team which shall include, at a minimum: • Data Scientists.

Checklist – Business Intelligence and Analytics Domain

BIA.MQ.3	Has the entity defined and implemented practices to manage and govern the BIA processes?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Data Engineers. - Visualization Engineers. The operating model must be approved by the entity's authority holder and remain valid.
	Evidences of training courses & awareness campaigns conducted.	- A document must be attached showing the following: - Proofs of all conducted training courses. - Proofs of all conducted awareness campaigns.
	The approved User Acceptance Test (UAT) Documents.	- A document must be attached showing the following, at a minimum: - The approved plan(s) to conduct UATs. - The approved report(s) on UATs. The plan and reports must be approved by the entity's authority holder and remain valid
	The approved outcomes as Reports & Dashboards produced for The Business Units.	- A document must be attached showing the following: - The reports which were generated & approved for each business unit. - The Dashboards which were generated & approved for each business unit. - Proofs of fully activating self-service analytics, covering both business intelligence and artificial intelligence/machine learning (AI/ML). The outcomes must be approved by the entity's authority holder and remain valid
	The Capacity planning document.	- The Capacity Planning document must be attached showing the following, at a minimum: - The Current Status Analysis: Analyzing the current BIA activities capacity. - The Future Status Analysis: Analyzing the expected demand for BIA services. - The Requirements: Detailing the specific resources required to satisfy the expected BIA Service demands, including hardware devices, software, and employees. - Capacity Gaps: Identifying the gaps between the current & future capacities / capabilities, and defining strategies to fill the gaps. - Resource Allocation: Documenting the process of allocating resources to support the entity's BIA activities, including capacity / capability allocation & resource management.
Level 4: Managed	The Monitoring Report on the effectiveness of practices and processes for managing and governing business intelligence and analytics	The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of practices and processes for managing and governing business intelligence and analytics based on pre-defined and identified KPIs and indicator cards.

Checklist – Business Intelligence and Analytics Domain

BIA.MQ.3	Has the entity defined and implemented practices to manage and govern the BIA processes?	
Levels	Acceptance Evidence	Acceptance Criteria
	through pre-defined key performance indicators (KPIs).	- Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values

Checklist – Business Intelligence and Analytics Domain

BIA.MQ.3	Has the entity defined and implemented practices to manage and govern the BIA processes?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The monitoring Report on the effectiveness of training and awareness sessions conducted through pre-defined key performance indicators (KPIs).	The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of conducted training and awareness sessions based on pre-defined and identified KPIs and indicator cards including, at a minimum: • Number of training and awareness sessions conducted. • Other optional indicators include: • The degree of satisfaction of the participants or target audience upon completion of the training course or awareness campaign. • The percentage increase in participation in subsequent events or activities, and the percentage of people who successfully completed the training course compared to the total number of participants. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.3	Has the entity defined and implemented practices to manage and govern the BIA processes?	
Levels	Acceptance Evidence	Acceptance Criteria
	- Performance Measurement Report for the Business Intelligence and Analytics Team.	The report should include the following: • Team Performance Indicators: This includes tracking the team's performance through specific indicators such as execution level, quality of work produced, and adherence to timelines. • Goal Achievement: The report analyzes the team's achievement of pre-defined goals, such as the development and implementation of specific analytics. • Data and Analytics Quality: The quality of the data used in the analytics and the accuracy of the resulting insights are evaluated. • Work Efficiency: The overall work efficiency of the team is estimated by analyzing completed tasks and the effective use of tools and techniques. • Feedback and Satisfaction: The report may also include surveys of feedback from clients or internal users to assess their satisfaction and measure the quality of the services provided. • These are just examples, and the content of a Business Intelligence and Analytics Team Performance Measurement Report may vary depending on the needs and goals of the organization.
Level 5: Pioneer	- Establishment of Business Intelligence and Analytics Center Document.	A document must be attached to confirm the establishment of the Business Intelligence and Analytics Center within the entity. The document should include the center's name, objectives, and responsibilities.
	- The continuous review and improvement of business intelligence and analytics management and governance practices.	A report must be attached showing the Reviews, Continuous Improvement & Governance Plan for BIA practices including the following, at a minimum: • The Review process: It includes the stakeholders' roles & responsibilities, e.g., the data science / BIA team, business & IT stakeholders. Review methods & tools may be referenced, e.g., Data Collection & Data Analysis methods & tools. • Schedule: The timetable for conducting the review. The schedule may be based on a specific timeframe, e.g., Quarterly, semiannually, or annually, or it may be based on specific incidents/events, such as the completion of a major project. • Metrics: The measures used to assess the effectiveness of BIA Practices & BIA Governance, which may include: • Performance Metrics, such as the accuracy of the reports & dashboards. • Compliance Metrics, such as conformity with Data Security & Privacy Policies. • Reporting & Communication: Review reporting & communication procedures. This may include routine reports sent to the Data Science/BIA team and other business & IT stakeholders. • The improvements made to business intelligence and analytics management and governance practices.

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.3	Has the entity defined and implemented practices to manage and govern the BIA processes?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The continuous review and Improvement of Business Intelligence and Analytics Team Performance.	The document should include, at a minimum, the following: • Team Performance Review: Regularly collect and analyze data related to team performance, utilizing any previous measurements of team performance. • Identify Strengths: Identify areas of strength in performance to enhance and/or leverage them in other tasks or projects. • Identify Areas for Improvement: Identify weaknesses in performance and determine areas that need improvement. • Enhance Training and Development: Training and development opportunities provided to team members to enhance their skills and capabilities in the field of business intelligence and analytics based on regular performance reviews. These opportunities may include workshops, training courses, and individual mentoring.
	- The Updated Capacity Planning document.	- An updated document must be attached showing Capacity Planning including at a minimum: • The Current Status Analysis: Analyzing the current BIA activities capacity. • The Future Status Analysis: Analyzing the expected demand for BIA services. • The Requirements: Detailing the specific resources required to satisfy the expected BIA Service demands, including hardware devices, software, and employees. • Capacity Gaps: Identifying the gaps between the current & future capacities / capabilities, and defining strategies to fill the gaps. • Resource Allocation: Documenting the process of allocating resources to support the entity's BIA activities, including capacity / capability allocation & resource management.
	- The Revised Demand Management Process.	- The revised process document of BIA Service Demand Management must be attached showing the following at a minimum: • The review results summary of the Demand Management Process. • Demand Analysis: Updates on the process of analyzing the BIA service demand, including request volume, frequency, and complexity. • Request Prioritization: Updates on the process of prioritizing BIA service requests, including updates on the criteria that will be used to prioritize each request. • Resource Allocation: Updates on the process of allocating resources to support the BIA service demand. • Communication: Updates on the process of communicating the BIA service demand status to the stakeholders, and about the performance of the Demand Management process.

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.3	Has the entity defined and implemented practices to manage and govern the BIA processes?	
Levels	Acceptance Evidence	Acceptance Criteria
		Governance & Compliance: Updates on the Governance & Compliance process to implement this approved process for BIA service Demand Management.

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.4	Has the entity implemented the right tools, technologies, and skills to empower users and support the implementation of the BIA use cases?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- The list of BIA tools.	- A document must be attached covering the list of tools used for the entity's BI activities. For each tool being used, the following must be indicated at a minimum: - The name of the tool. - The users or the target audience.
	- The list of reports.	- A document must be attached covering: - The list of names of BIA report which were generated. - Complete copies of the BIA reports.
Level 2: Defined	- The list of business units which use the BIA technology tools.	- A document must be attached covering: - A list of names of the business units that use BI technology tools. - Details of business units that use BI technology tools, which include, at a minimum: - The name of the business unit. - The name of the tool utilized. - The version of the tool. - The purpose of the usage. - The Stakeholders Cooperation to provide the Semantic Layer's details.
Level 3: Activated	- The List of Users with Roles and Privileges.	- A document containing a comprehensive list of users must be attached, including the following information:

Checklist – Business Intelligence and Analytics Domain

BIA.MQ.4	Has the entity implemented the right tools, technologies, and skills to empower users and support the implementation of the BIA use cases?	
Levels	Acceptance Evidence	Acceptance Criteria
		• Usernames and job roles: Specify each user's username and job role within the entity. • Access and privileges: Define the level of access and privileges granted to each user in the systems, tools used for data analysis, and the application of artificial intelligence and machine learning models. • Tool and platform permissions: Clarify the tools or platforms each user is authorized to access and use, such as programming languages (Python and R), libraries (Pandas and Numpy), and platforms (Anaconda and Jupyter). • Role and privilege updates: Identify any recent changes made to job roles or privileges to ensure continuous updates. The document must be up-to-date and accurately reflect all active users, their current roles, and privileges. System screenshots must be attached as evidence of the actual roles and privileges.
	- The Approved Architecture & Documentation for Advanced Analytics.	- A document must be attached describing the Approved Architecture & the Approved Documentation for the entity's Advanced Analytics, which may include: • The Advanced Analytics Architecture, including technologies required to support Advanced Analytics. • Data Storage: Data Storage solutions required to store and manage large data quantities to be used in Advanced Analytics. • Data Processing: Processing Algorithms & Technologies used to analyze & model data within an Advanced Analytics system. • Analytics Applications: The applications & tools used to create & deploy analytical models & insights. • Governance: The Processes & Policies required to control the use of Advanced Analytics within the entity, including Data Security, Data Privacy, and Compliance Requirements. • The Implementation Plan: The steps required to implement the Advanced Analytics system within the entity, including timetables & requirements such as budgets & resources. - The Architecture & Documentation for Advanced Analytics must be approved by the entity's authority holder and remain valid.
	- Advanced Analytics and Communication Project Management Documents.	• The following documents should be included: • Documents for advanced analytics project management: This includes typical project management elements such as planning, project scheduling, and governance, with a focus on technical planning for data collection, advanced analytics, and predictive models. It should also detail technical aspects related to data quality, validity, and cleaning, while considering the requirements of advanced technical infrastructure. • Communication documents: This involves project status updates and reports, including progress in developing analytical models and

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.4	Has the entity implemented the right tools, technologies, and skills to empower users and support the implementation of the BIA use cases?	
Levels	Acceptance Evidence	Acceptance Criteria
		outcomes, sent to stakeholders such as executive sponsors, business users, and IT teams. - Document management and sharing mechanisms: The mechanisms for managing and sharing technical documentation and analytical data must be clarified, using advanced data management systems to ensure organized and secure access to datasets and analytical models. - AI ethics considerations: In planning and analysis, ethical considerations related to the use of artificial intelligence and advanced analytics must be included, such as privacy protection, ensuring fairness, and maintaining transparency in the development and use of analytical models.
	The Approved Advanced Analytics Models Documents.	- A document must be attached listing all models developed for Advanced Analytics, model verifications and model approvals for usage. For each Advanced Analytics Model, the following must be documented, at a minimum: - The purpose of the Model. - The data sources used. - The methodology used. - Verification, Validation, and testing processes. The models must be approved by the entity's authority holder and remain valid
Level 4: Managed	Report on the Effectiveness Monitoring of Business Intelligence and Analytics Tools and Techniques through Pre-defined Key Performance Indicators.	- A report on the effectiveness monitoring of business intelligence and analytics tools and techniques must be attached, and it may include the following: - Key Performance Indicators: Predefined key performance indicators and actual measurements for the adoption and utilization of business intelligence and analytics tools. These indicators may include the number of participating users, data processing volume, response time, and performance. - Tool and Technique Usage: Evaluation of the extent of usage of the adopted tools and techniques for data analysis and value extraction. This may include details on usage ratios and distribution among different departments and teams within the organization. - Results and Analysis: The results, analysis, and insights achieved through the use of business intelligence and analytics tools. - Recommendations and Improvements: Recommendations for improving the usage of tools and techniques and enhancing their adoption within the organization. Areas for improvement are identified, and appropriate guidance is provided to enhance effectiveness and optimize the benefits of business intelligence and analytics tools. - Success Evaluation: Evaluation of the success of adopting and utilizing business intelligence and analytics tools. Results are measured against expected objectives and outputs, and an analysis is provided on the achieved benefits and ongoing challenges.

Checklist – Business Intelligence and Analytics Domain

BIA.MQ.4	Has the entity implemented the right tools, technologies, and skills to empower users and support the implementation of the BIA use cases?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 5: Pioneer	- Document for Continuous Adoption of Technologies, Tools, Frameworks, and Features.	- The document for continuous adoption should include the following: • A list of new tools and technologies that have been evaluated or tested and identified. • Advanced technologies (such as Spark, TensorFlow, and PyTorch) that have been integrated into the artificial intelligence/machine learning environment. • A list of advanced capabilities, such as tools and engineering features, in artificial intelligence/machine learning that are utilized for complex processing and reusability. • A list of tools and techniques used in artificial intelligence/machine learning operations for comprehensive management of the artificial intelligence/machine learning lifecycle.
	- The Continuous Improvement Report of the BIA and Advanced Analytics Technology Solutions including the Proof of Concept (POC) Roadmap.	- A document must be attached for the new technological solution's roadmap of advanced analytics (POC), which is a detailed plan for testing and evaluating new technologies or tools in the advanced analytics field. This is to prove the existence & implementation of a continuous improvement mechanism. The Report must include the following, at a minimum: • The Scope: Specifying the scope of the new technological solution's POC, including the technologies being tested, data sources, and the target audience. • The Success Criteria: Identifying the success criteria and metrics that will be used to assess success. • The Timeline: Setting realistic timetables, including start & end dates and milestones. • Resources: Determining the resources needed to implement the new technological solution's POC, including technologies, data, employees, and budget. • Risks & Challenges: Identifying potential risks & challenges associated with the new technological solution's POC and develop a mitigation plan. • The Communication Plan: Developing a communication plan to keep stakeholders informed about the progress and the results of the new technological solution. • Next Steps: Determining the next steps following a POC, such as upscaling the new technological solution, performing extra tests, or additional implementations.
	- A Report on the Proof of Concept (POC) Results.	- A report must be attached containing the POC results of each new technological solution, including, at a minimum:

Checklist – Business Intelligence and Analytics Domain		
BIA.MQ.4	Has the entity implemented the right tools, technologies, and skills to empower users and support the implementation of the BIA use cases?	
Levels	Acceptance Evidence	Acceptance Criteria
		• An Executive Summary: A brief overview of the main objectives & key results. • The Methodology: A Description of the methodology used in conducting the POC & performing the periodic tests of the technological solution. • The Results: A detailed analysis of the POC results & the periodic testing results, including the solution's strengths & weaknesses, predictions accuracy, and any limitations or issues encountered. • Recommendations: Any insights or recommendations derived from the results. • The Conclusion: A conclusion that summarizes the POC results & highlights the business implications. • The Future Directions: A discussion of the project's potential next steps, including any recommendations for further development, testing, or deployment. • Appendices: Supporting materials such as technical documentation, programming code samples, data visualizations, and interfaces.

8.2.10. Data Value Realization Domain

Checklist – Data Value Realization Domain		
DVR.MQ.1	Has the entity developed a plan to identify, document and realize its data revenue generation potential and implement data-related cost optimization initiatives and use cases?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- The Existing List of Data Value Realization (DVR) Activities.	- A document must be attached covering a Proof-of-Concept (POC), or other temporary tasks performed as practices that support Data Value & Benefit Realization within the entity. The document must include the following: • The currently existing DVR Domain practices. • A separate description for each activity including, at a minimum: • The name of the activity. • The purpose of the activity. • The achieved or expected output of the activity.
Level 2: Defined	- The Data Value Realization (DVR) plan.	- The recent DVR Plan, approved by the entity's authority holder must be attached to activate data revenue generation capabilities (Profitable revenue from data) and activate data based cost-reduction initiatives. The plan shall include the following, at a minimum: • A roadmap that includes the activities and milestones for the DVR use cases. The activities shall incorporate what is needed to achieve this Domain's specifications, at a minimum. • The assignment of the required resources & budget allocation to manage the implementation of the DVR use cases.
	- The List of Identified Use Cases for Both Revenue Generation & Cost Optimization.	- A document must be attached covering the DVR use cases. Each use case should be documented with the following details, at a minimum: • Name of use case. • Type of use case e.g.: • Data Revenue Generation Use Cases – data or Data Products which generate revenue for the entity. • Cost Saving Use Cases – Data related cases which will directly or indirectly contribute to reducing expenses and achieving greater efficiency. • The stakeholders required to implement the use cases, the official who will lead the use case, and the target beneficiary who will benefit from the implementation of the use case. • A list of business requirements needed to implement the use cases. • Data sources and required data fields.

Checklist – Data Value Realization Domain		
DVR.MQ.1	Has the entity developed a plan to identify, document and realize its data revenue generation potential and implement data-related cost optimization initiatives and use cases?	
Levels	Acceptance Evidence	Acceptance Criteria
		The technology required to implement the use cases.
	A Document Explaining the Payback Period and Return on Investment (ROI) for Each Identified Use Case.	- A document must be attached containing the following: - An estimation of the payback period and the ROI for each DVR use case.
Level 3: Activated	A Report on DVR Monitoring & Maintenance.	A report on the status of monitoring and maintaining data value realization use cases must be attached, and it must include, the following at a minimum: The monitoring and maintenance of the DVR use cases must include the following, at a minimum: - Measuring and verifying/validating the KPIs (ROI & Payback Period) against the projected income values in the DVR & Income Plan. - Developing Change Request (CR) documents to accommodate change requirements from the end users. - Reporting defects & malfunctions in the implemented use cases.

Checklist – Data Value Realization Domain		
DVR.MQ.1	Has the entity developed a plan to identify, document and realize its data revenue generation potential and implement data-related cost optimization initiatives and use cases?	
Levels	Acceptance Evidence	Acceptance Criteria
	- Implementation Status Report of the Data Value Realization Plan	- The entity must attach a report on the implementation status of the Data Value Realization Plan and its roadmap, including the following, at a minimum: • Initiatives and projects status: Identifying the status of each initiative or project (started, in progress, completed, or delayed), along with clarification of any delays or challenges. • Progress percentages: Providing the progress percentages of activities and milestones in the plan and roadmap, with clear details on the actual activities that have been completed. • Supporting evidence: Attaching proof of achieved progress/completion, such as reports, photos, documents, or meeting minutes that support the implementation status.

Checklist – Data Value Realization Domain		
DVR.MQ.1	Has the entity developed a plan to identify, document and realize its data revenue generation potential and implement data-related cost optimization initiatives and use cases?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Organizational Structure for Data Value Realization (DVR) Activities.	- The documented organizational structure, approved by the entity's authority holder, for Data Value Realization activities must be attached, including at a minimum the following: • Job roles and responsibilities. • Approved job descriptions for each of these roles. • Authorities: reviews, approvals, and decision-making.

Checklist – Data Value Realization Domain		
DVR.MQ.1	Has the entity developed a plan to identify, document and realize its data revenue generation potential and implement data-related cost optimization initiatives and use cases?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 4: Managed	- The Monitoring Report of the DVR Use Cases with Pre-defined KPIs.	- The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of DVR Use Cases based on pre-defined and identified KPIs and indicator cards, covering the following: • The number of developed data products. • The number of data or data product revenue requests. • The payback period for DVR use cases. • Return on Investment (ROI) for DVR use cases. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values

Checklist – Data Value Realization Domain		
DVR.MQ.1	Has the entity developed a plan to identify, document and realize its data revenue generation potential and implement data-related cost optimization initiatives and use cases?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Monitoring Report of the DVR Activities & Plan with Pre-defined KPIs.	- The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of DVR plan and activities based on pre-defined and identified KPIs and indicator cards, covering the following: - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive polarity: Higher indicator value is the target, negative polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- Review & Continuous Improvement Document of the DVR Plan.	- The entity must attach an updated report, approved by the entity's authority holder demonstrating continuous improvement of the DVR domain plan based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: • Reviews conducted. • Results of each review.

Checklist – Data Value Realization Domain		
DVR.MQ.1	Has the entity developed a plan to identify, document and realize its data revenue generation potential and implement data-related cost optimization initiatives and use cases?	
Levels	Acceptance Evidence	Acceptance Criteria
		Improvements implemented (with supporting documents).
	The Revised & Updated DVR KPIs.	- A document must be attached including the following, at a minimum: - The revised & updated DVR KPIs. - Each indicator card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
	Evidences of New Partnerships (e.g., MoU, jointly developed use cases or products, etc.).	- A document must be attached proving new partnerships, which may contain proofs such as: - Memorandum of Understanding (MoU): In the event of signing a Memorandum of Understanding, a copy of the MoU must be attached. - Jointly Developed Use Cases or Data Products: If the partnership contributed to the development of new use cases or products, they must be documented and described. There must be a brief

Checklist – Data Value Realization Domain		
DVR.MQ.1	Has the entity developed a plan to identify, document and realize its data revenue generation potential and implement data-related cost optimization initiatives and use cases?	
Levels	Acceptance Evidence	Acceptance Criteria
		explanation of each use case and each data product, its purpose and the value it may provide.

Checklist – Data Value Realization Domain		
DVR.MQ.2	Has the entity implemented practices to support a data revenue generation process?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- The Existing Practices Related to Supporting the Data Revenue Generation Process.	- A document must be attached containing the current practices which support data revenue generation including, at a minimum: A list of the current activities (reports and/or dashboards...etc.) related to the DVR Domain practices.
Level 2: Defined	- The Defined Pricing Scheme.	- A document must be attached containing: A suitable Pricing Model for any data and for any data product that's expected to generate revenue.
	- The Data or Data Product Price Calculation.	- A document must be attached containing the total expense calculation for each data or Data Product which is expected to generate revenue. The total cost shall include the following at a minimum: - The Data Collection Cost – The total of the costs incurred for collecting, cleansing, and curating data. - The Data Development Cost – The total of the costs incurred for developing analytical models, data visualizations and other value-added services provided on top of the collected data.
	- The Adopted / Approved Charging Model for Each Data or Data Product.	- A document must be attached containing the approved Charging Calculation Model for each data or Data Product that's expected to generate revenue. - Here are examples of Charging Calculation Models, but not limited to: - The Subscription Model. - The Consumption Based Model. - The Freemium / Premium Model. - The One Time Fee Model. The fee calculation model(s) must be approved by the entity's authority holder and remain valid.

Checklist – Data Value Realization Domain		
DVR.MQ.2	Has the entity implemented practices to support a data revenue generation process?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 3: Activated	- Evidence of Revenue Generation Requests Submitted to the Internal DMO at the Entity.	- A document must be attached containing proofs of requests sent to the DMO at the entity for revenue or income generation from data or from data products. - Each request shall include the following, at a minimum: • The Description of the data or the Data Product. • The Documentation of the Data Product Pricing Scheme / Model & the Service Pricing Scheme / Model. • The Proposed Charging Model. • The Proposed Final Unit Price. • The Justification if the Final Unit Price does not follow the Cost Recovery Pricing Scheme.
Level 4: Managed	- The Monitoring Report of the Data Revenue Generation Process with Pre-defined KPIs.	- The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of the Data Revenue Generation Process based on pre-defined and identified KPIs and indicator cards, covering the following, at a minimum: • The number of Data Products that generated revenue. • Total revenue generated from offering data or Data Products. • The total cost saved from the implemented Cost Saving Use Cases. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target).

Checklist – Data Value Realization Domain		
DVR.MQ.2	Has the entity implemented practices to support a data revenue generation process?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The continuous Improvement Report of the Data Revenue Generation Process.	- The entity must attach the continuous improvement report of the data revenue generation process based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: - Innovation or improvement mechanisms used to continuously enhance and develop the revenue generation process - Documents of the Periodic reviews and results of the Pricing Model, Price Calculation for data or data products, and the Charging Fee Calculation Model. - New or innovative models developed for pricing, fee calculation, and revenue generation. - The improvement recommendations or updates on the data revenue generation process based on innovation/improvement and review results.

8.2.11. Open Data Domain

Checklist – Open Data Domain		
OD.MQ.1	Has the entity defined, established, and implemented a plan to identify and coordinate the publishing of its Open datasets?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- The existing list of Open Datasets.	- A document must be attached covering the current list of open datasets including the following, at a minimum: - For each existing open dataset, the following information must be provided, at a minimum: • Name: The name of the open dataset. • Description: A brief description of each open dataset, including its source and any related information. • Download Links: The download link of each open dataset.
Level 2: Defined	- The Approved Open Data Framework.	- Document must be attached including the following, at a minimum: • The approach/methodology used to make open data available to the public. The framework must be approved by the entity's authority holder.
	- The Approved Open Data Plan.	- The recent OD plan, approved by the entity's authority holder, must be attached, including the following at a minimum: • A roadmap that includes activities milestones for the implementation of OD initiatives. The activities shall include what is necessary to achieve the specifications of this Domain, at a minimum. • Allocation of the required resources & budget to manage the implementation of OD initiatives.
	- The OD Management structure.	- An Open Data Management Structure document must be attached including, at a minimum: • The roles & responsibilities. • The compliance audit framework.
	- The Developed and Approved Plan for Change Management (Including awareness campaigns).	- A document must be attached containing the change management plan that has been developed & approved including, at a minimum: • The OD activities awareness campaigns plan including the following, at a minimum:

Checklist – Open Data Domain		
OD.MQ.1	Has the entity defined, established, and implemented a plan to identify and coordinate the publishing of its Open datasets?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The usage of open data, and its various positive social & economic benefits. - Promoting the entity's open data & the related activities. The plan must be approved by the entity's authority holder and remain valid.
	The Developed and Approved Plan for Change Management (Including Training Programs).	- A document must be attached containing the change management plan that has been developed & approved including: - Training objectives: Clarifying goals such as enabling employees to implement open data policies and improving efficiency in managing them. - Target groups: Specifying the training audience and their job levels. - Training content: Including open data definition, publishing policies, tools and technologies, data classification, impact and risk assessment, and privacy assurance. - Training schedule: Defining the training dates and phases. The plan must be approved by the entity's authority holder and remain valid.
Level 3: Activated	The Open Data Plan Implementation Status Report.	- The entity must attach a report of the open data plan and roadmap implementation status, including the following, at a minimum: Initiatives and projects status: Identifying the status of each initiative or project (started, in progress, completed, or delayed), along with clarification of any delays or challenges. Progress percentages: Providing the progress percentages of activities and milestones in the plan and roadmap, with clear details on the actual activities that have been completed. Supporting evidence: Attaching proof of achieved progress/completion, such as reports, photos, documents, or meeting minutes that support the implementation status.
	Evidence of Submission of the Annual Compliance Report to NDMO-SDAIA.	The entity must attach the Annual Compliance Report submitted to NDMO-SDAIA and attach the evidence of the submission.

Checklist – Open Data Domain		
OD.MQ.1	Has the entity defined, established, and implemented a plan to identify and coordinate the publishing of its Open datasets?	
Levels	Acceptance Evidence	Acceptance Criteria
	- Assignment Decisions / Appointees to Job Roles.	- A document must be attached including the hiring / assignment decisions for the following roles including job descriptions: - Open Data & Information Access Officer (ODIAO). - Business Data Executive (BDE). - Business Data Steward.
	- Evidence of Implementation of the Change Management Program (The conducted training courses and the launched awareness campaigns related to Open Data).	- A document should be attached that includes the following: - Evidence of the implementation of training courses related to Open Data. - Evidence of the launch of awareness campaigns related to Open Data.
Level 4: Managed	- The Monitoring Report on the Effectiveness of the Open Data Plan through Predefined Key Performance Indicators (KPIs).	- The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of the Open Data Plan based on pre-defined and identified KPIs and indicator cards. - Each indicator card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.).

Checklist – Open Data Domain		
OD.MQ.1	Has the entity defined, established, and implemented a plan to identify and coordinate the publishing of its Open datasets?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The periodic reviews and improvements of the open data plan.	- The entity must attach an updated report, approved by the entity's authority holder demonstrating continuous improvement of the open data domain plan based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: • Reviews conducted. • Results of each review. • Improvements implemented (with supporting documents).

Checklist – Open Data Domain		
OD.MQ.2	Has the entity defined, established, and implemented a process to support the identification of Open Data (OD)?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents.
Level 1: Establishing	- The Existing Practices for OD Identification.	- A document must be attached, explaining: The Current OD Identification Practices.
Level 2: Defined	- The Defined Process Documentation for Managing the Lifecycle of Open Data.	- A document must be attached containing the Open Data Lifecycle Management Processes including the following, at a minimum: - Processes to identify public datasets to be published by the entity. - Processes to ensure that datasets are published and maintained to their appropriate format, timeliness, comprehensiveness, and overall high quality and ensure the exclusion of any Confidential data. - Processes for gathering feedback, analyzing performance at the entity level, and improving the overall Open Data national impact.
	- The Defined Process Documentation for Identifying Open Data.	- A document must be attached containing the Open Data Identification Process including the following, at a minimum: - Identifying and documenting all data classified as 'Public' and prioritizing each dataset included under open data. - Evaluating the identified datasets to determine whether to be published as open data or not. - Determining whether the combination of any publicly available data and the data to be published would constitute an unauthorized disclosure of Personal Information, or any other Security or privacy risk or threat. The process must be approved by the entity's authority holder and remain valid.

Checklist – Open Data Domain		
OD.MQ.2	Has the entity defined, established, and implemented a process to support the identification of Open Data (OD)?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Process of Evaluating the Value and Impact of Open or Public Datasets.	- Should include a document that outlines the process for assessing the estimated value and potential impact of open or public datasets, which should include, at a minimum, the following: • Steps and methods for analyzing the value of each open dataset from different dimensions such as economic (e.g., ROI), social, and environmental dimensions. • Steps and methods for evaluating the potential impact after sharing open or public datasets, such as increasing transparency, improving decision-making processes, and enhancing research and innovation. • Risk assessment and mitigation methods for identifying potential risks associated with open datasets, such as security threats, data breach, privacy concerns, Data Quality (DQ) issues, intellectual property violations, etc. The process must be approved by the entity's authority holder and remain valid.
Level 3: Activated	- The OD Identification Process Implementation Status Report.	- A report must be attached showing the implementation status of the Open Data identification process.
	- The List of Identified Open Datasets with the Assigned Priorities.	- A document must be attached containing the list of public datasets considered to be published as open data, with the classification & prioritization information for each dataset. - For each dataset, the following information must be provided, at a minimum: • Name: The name of the dataset. • Description: A brief description of each dataset, including its source and any related information. • Size: The size of each dataset in terms of the number of records or file size. - The list must be approved by the entity's authority holder and remain valid.
	- The Identified & Documented Metadata for the Open Datasets.	- A document must be attached containing the identified & documented metadata of the open datasets including, at a minimum: - The necessary metadata for each open dataset, to easily identify, describe and search for it once published. The metadata for each open dataset may include several elements such as: • Dataset name.

Checklist – Open Data Domain		
OD.MQ.2	Has the entity defined, established, and implemented a process to support the identification of Open Data (OD)?	
Levels	Acceptance Evidence	Acceptance Criteria
		• A brief description of the dataset. • Publishing entity. • Language. • Time period. • Source link. • Regular updates (e.g., weekly, monthly, quarterly, annually, etc.). • Spatial coverage (e.g., city/cities). • Creation date. • Update date. • Tags/Keywords.
	- Value and Impact Assessment Report for the Identified Open or Public Datasets.	- A value and impact assessment report for the identified open or public datasets to be published must be attached, which should include, at a minimum, the following: • Results of evaluating the value and impact of the identified datasets to decide whether or not to publish them as Open Data. • Risk assessment report for identified potential risks associated with publishing the open datasets.

Checklist – Open Data Domain		
OD.MQ.2	Has the entity defined, established, and implemented a process to support the identification of Open Data (OD)?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 4: Managed	- The Monitoring Report of OD Identification & Prioritization Processes with Pre-defined KPIs.	- The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of OD Identification Processes based on pre-defined and identified KPIs and indicator cards covering the following at a minimum: • Number of identified and prioritized open datasets. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values.
Level 5: Pioneer	- The Continuous Improvement Report Showing the Documented Periodic Reviews & Outcomes of the OD Identification Processes and the Implemented Automation.	- The continuous improvement report must be attached proving the periodic reviews & outcomes of the OD identification processes and the implemented automation processes based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: • The document of periodic reviews & results which were documented for the OD identification processes and the implemented automations.

Checklist – Open Data Domain		
OD.MQ.2	Has the entity defined, established, and implemented a process to support the identification of Open Data (OD)?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The continuous improvement mechanisms of the OD identification processes and the implemented automations. - The processes which were implemented & automated to support OD identification.

Checklist – Open Data Domain		
OD.MQ.3	Has the entity defined, established, and implemented a process to support publishing its Open Datasets?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- The Existing Practices for Publishing Open Datasets.	- A document must be attached, explaining: The current practices related to Publishing Open Datasets.
Level 2: Defined	- The Defined Process Documentation for Publishing Open Data.	- A document outlining the Open Data Publishing Process must be attached showing steps to ensure that datasets are published and maintained to their appropriate format, timeliness, comprehensiveness, and overall high quality and ensure the exclusion of any Confidential data.
	- The Defined Process Documentation for Open Data Maintenance.	- A document outlining the Open Data Maintenance Process must be attached showing activities including, at a minimum the following: - Regular update and documentation of changes to its published Open Datasets and associated metadata whenever changes occur. - Continuous review of the published Open Datasets to ensure they meet the defined regulatory requirements. - Maintenance of data traceability by documenting data provenance and maintaining versioning history of the datasets. The process must be approved by the entity's authority holder and remain valid.
Level 3: Activated	- Status Report on the Implementation of the Open Data Publishing Process.	- The report must be attached showing the implementation status of the open data publishing process.

Checklist – Open Data Domain

OD.MQ.3	Has the entity defined, established, and implemented a process to support publishing its Open Datasets?	
Levels	Acceptance Evidence	Acceptance Criteria
	- Evidences of Published Datasets on the Saudi Open Data Platform.	- The proof document should include the datasets published on the National Open Data Platform under the Open Data License in the Kingdom of Saudi Arabia, as outlined in the Open Data Policy issued by NDMO-SDAIA. At a minimum, it should include the following: - For each dataset that's currently published on the National Open Data Platform, the following must be documented, at a minimum: • Name: The name of the open dataset. • License data. • Description: A brief description including its source and any related information. • Size: The size in terms of the number of records or file size. • Format: e.g.: CSV, JSON, or XML. • Download Links: The download link. • Publishing Date: The date the open dataset was first published. • Update Date: The last update date. • Usage and downloads statistics.
	- Evidences of Feedback / Comments Received on OD.	- A document must be attached containing proofs that there were feedback/comments on the open datasets published on the Open Data Platform. In case there is no feedback/comments received, proof must be attached.
	- Evidence of Formats Used to Standardize Open Datasets in Machine Readable Form.	- A document must be attached showing the formats of the published open datasets, such as CSV, JSON, or XML, and instructions on how to use the open dataset according to its published format.
	- Evidence of Data Standards Applied on Open Datasets to Ensure High Data Quality (DQ).	- A document must be attached showing evidence of the data standards applied on the open datasets to ensure high data quality. Including the following standards at a minimum: • Completeness (Data Completeness): (The extent to which data records are complete). • Uniqueness (Data Uniqueness): (The extent of data record repetition). • Timeliness (Data Timeliness): (How recent and timely the data is). • Validity (Data Validity): (The extent to which records conform to defined formats, types, and structures). • Accuracy (Data Accuracy): (The extent to which data values actual values).

Checklist – Open Data Domain		
OD.MQ.3	Has the entity defined, established, and implemented a process to support publishing its Open Datasets?	
Levels	Acceptance Evidence	Acceptance Criteria
		Consistency (Data Consistency): (The degree of data consistency across all operations and from various sources within the entity).
	- Open Data Maintenance Report.	- A report must be attached showing the Open Data maintenance process outcomes that include, at a minimum, the following: - Periodic data updates, and documentation of any changes made on the published open datasets and on the associated metadata (in the event of any changes). - Ongoing reviews of published datasets to ensure that they meet the specified regulatory requirements. - Evidence of data traceability by documenting data provenance and versioning history of the dataset.
	- The Open Data Register Containing Records of Open Data Activities and Published Open Datasets.	- A document must be attached that includes the following, at a minimum: - A record that includes artifacts related to Open Data Domain activities and decisions made during the data life cycle management. - A record that includes a list of all open datasets, reviews, and changes associated with them and their metadata.
Level 4: Managed	- The Monitoring Report of the OD Publishing Process with Pre-defined KPIs.	- The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of the OD Publishing Processes based on pre-defined and identified KPIs and indicator cards, covering at a minimum, the following: - The number of downloads per published Open Dataset. - The number of identified Open Datasets that have been published. - The number of updates performed on published Open Datasets. - Each indicator card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value.

Checklist – Open Data Domain		
OD.MQ.3	Has the entity defined, established, and implemented a process to support publishing its Open Datasets?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The Continuous Improvement Report of the OD Publication & Maintenance Practices and outcomes.	- The entity must attach the continuous improvement report of the OD publication & maintenance practices and outcomes, based on the results of the KPI measurements and relevant updates and developments in the domain, containing the following: - The documented periodic reviews & outcomes for the OD publication and maintenance practices. - The continuous improvement mechanisms of the OD publication and maintenance practices. - Regular reviews and updates of published open datasets and linked metadata to ensure compliance with the latest versions and standards. - Documented changes to open data and metadata when necessary to ensure transparency and clear tracking of modifications. - Impact assessment results for the published open datasets.

8.2.12. Freedom of Information Domain

Checklist – Freedom of Information Domain		
FOI.MQ.1	Has the entity defined and established a plan to address its compliance with the requirements of the Freedom of Information (FOI) Regulations?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents
Level 1: Establishing	- The Existing FOI Practices.	- The entity must attach a report on the current practices in the FOI Domain containing implementation evidences of these practices.
Level 2: Defined	- The Defined & Approved FOI Implementation Plan & Roadmap.	- The entity must attach the approved FOI Domain implementation plan and roadmap including the following, at a minimum: - A roadmap that includes the activities and milestones for the achievement of full compliance with the FOI regulations published by NDMO-SDAIA. The activities shall incorporate what is needed to achieve this Domain's specifications, at a minimum. - The assignment of the required resources & budget allocation to achieve full compliance with the FOI regulations published by NDMO-SDAIA.
Level 3: Activated	- The FOI Plan Implementation Status Report.	- The entity must attach a report of the FOI Plan implementation status, including the following, at a minimum: Initiatives and projects status: Identifying the status of each initiative or project (started, in progress, completed, or delayed), along with clarification of any delays or challenges. Progress percentages: Providing the progress percentages of activities and milestones in the plan and roadmap, with clear details on the actual activities that have been completed. Supporting evidence: Attaching proof of achieved progress/completion, such as reports, photos, documents, or meeting minutes that support the implementation status.
	- The Assigned Open Data & Information Access Officer (ODIAO).	- The entity must attach the Open Data & Information Access Officer (ODIAO) employment decision letter, with the roles and responsibilities stated.

Checklist – Freedom of Information Domain

FOI.MQ.1	Has the entity defined and established a plan to address its compliance with the requirements of the Freedom of Information (FOI) Regulations?	
Levels	Acceptance Evidence	Acceptance Criteria
	- FOI Awareness.	- The entity should attach a report proving its implementation of awareness campaigns in FOI, with the aim of instilling a culture of transparency and promoting it, and raising awareness of the policy of FOI issued by the NDMO-SDAIA and the right to access public information. Awareness campaigns should include, at a minimum, the following: • Raising awareness among employees involved in the processing of FOI requests to understand the main obligations and requirements of the FOI policies issued by the NDMO-SDAIA. • Raising awareness about the FOI principles and their application to the rights of beneficiaries.
Level 4: Managed	- The Monitoring Report on the Entity's FOI Plan & Activities with Pre-defined Key Performance Indicators (KPIs).	- The entity must attach an updated report, approved by the entity's authority holder on monitoring the FOI plan based on pre-defined and identified KPIs and indicator cards. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description. • The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). • Indicator's Equation. • Measurement Unit (Percentage, Number / Quantity, etc.). • Baseline. • Target value. • Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). • Data sources used to calculate the indicator. • Data collection mechanism (manual/automated). • Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). • The current indicator value compared to the target value. • Indicator status (achieved/delayed/not achieved, etc.).

Checklist – Freedom of Information Domain		
FOI.MQ.1	Has the entity defined and established a plan to address its compliance with the requirements of the Freedom of Information (FOI) Regulations?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The report should also include: • Recommendations to improve performance based on the actual indicator values. • Supporting documents for the data used to calculate the indicator values
	- The Internal Audit Reports on the Entity's Compliance with the FOI Regulations.	- The entity must attach reports including the following: • The conducted internal audits of monitoring the compliance with the FOI Regulations published by NDMO-SDAIA. • The documented audit findings, submitted in a report to the Open Data & Information Access Officer (ODIAO). • The corrective actions applied in cases of non-compliance, with notifications to the regulatory authority or NDMO -As it stated-, and documentation of these improvements in the audit findings report.
Level 5: Pioneer	- The Continuous Improvement Report of the FOI Plan.	- The entity must attach an updated report, approved by the entity's authority holder presenting continuous improvement of the FOI domain plan based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: • Reviews conducted. • Results of each review. • Improvements implemented (with supporting documents).

Checklist – Freedom of Information Domain		
FOI.MQ.2	Has the entity defined and implemented the required processes for Freedom of Information (FOI)?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents.	- No required documents
Level 1: Establishing	- The Existing Processes for the FOI Requests & Responses.	- The entity must attach evidences of a previously done process(es) and response(s) to information request(s).
Level 2: Defined	- The Developed & Approved FOI Request Processes & Procedures Documentation.	- The entity must attach the developed and approved procedures and processes of FOI requests. The entity must design and document a standardized / unified process for information requests and develop procedures for managing, processing and

Checklist – Freedom of Information Domain

FOI.MQ.2	Has the entity defined and implemented the required processes for Freedom of Information (FOI)?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Developed FOI Process Guide & FAQs.	documenting requests for access to public information based on the FOI Regulations published by NDMO-SDAIA. - The entity must attach the developed FOI process guideline and answers to the Frequently Asked Questions (FAQs). - The guide must clarify the following, at a minimum: • The request preparation mechanism. • The request sending mechanism. • The response awaiting mechanism. • The response review mechanism. • The appeals mechanism (if required). • Moreover, the FAQs may include: • Common questions about the FOI process, requirements, timelines, and other info related to requesting information. Submitting FAQs can help clarify common inquiries and provide useful info for individuals seeking to submit FOI requests.
Level 3: Activated	- The Implementation / Adoption Status Report on the FOI Request Processes. - Evidences of Entity-wide Communication.	- The entity must attach a report on the FOI request process implementation status covering the following: • Granting access to a public information request(s). • Denying a public information access request(s). • Extending the time required to respond to specific requests. • Notifying the requestor(s) if the required information is available on the entity's website or is not within its specialty. - The entity must attach evidences for entity-wide communications and public publications, in alignment with the FOI Regulations published by NDMO-SDAIA, without contradicting the applicable regulations in the Kingdom of Saudi Arabia (KSA). The entity must publish the following information on its official government website or websites linked to it: • The Laws, regulations, instructions and regulatory decisions applicable to the entity / followed within the entity. • The entity's services provided with description detailing how to obtain access to those services. • The entity's organizational structure including the roles & responsibilities. • The entity's job vacancy information, except information of security or military job vacancies as determined by the security or military regulatory authorities or applicable KSA Regulations. • The entity's annual strategic and operational reports including the entity's financial statements.

Checklist – Freedom of Information Domain

FOI.MQ.2	Has the entity defined and implemented the required processes for Freedom of Information (FOI)?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The entity's general statistics, news and updates on its activities including the following, at a minimum: - The number of the entity's employees. - The year of the entity's establishment. - The number of the entity's services provided in the last year. - The entity's up-to-date activities' descriptions. - The projects provided by the entity as stated in the FOI Regulations regarding the risks which may affect people's lives, health and properties. The information must contain the contact details of persons with valid licenses granted by the entity including the following, at a minimum: - The names of the persons. - The postal addresses of the persons. - The e-mail addresses of the persons. - Information on projects offered or awarded by the entity as prescribed by the FOI Regulations regarding any risk that may affect people's lives, health or properties. The information must include the following, at a minimum: - The names of the recipients. - The execution periods. - The technical analysis. - The guidelines and leaflets that raise the people's awareness of their rights to the entity's FOI. - If the information above is not available or applicable, the entity must provide a justification with these evidences, and based on the FOI Regulations.
	- The Register of the Received Request Forms with the Responses.	- The entity must attach the prepared request forms for access to Public Information -whether paper or electronic specifying the required information to be provided by the Requestor. The required information must include the following, at a minimum: - Information about the Requestor including name, address, national ID. - Description of Public Information requested by the requestor. - Purpose behind the request for access to public information. - Legal basis for the request. - Notice delivery method to the requestor (e-mail, national address). - Date of the request.

Checklist – Freedom of Information Domain

FOI.MQ.2	Has the entity defined and implemented the required processes for Freedom of Information (FOI)?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Identified Public Datasets Shared Under the FOI Regulations.	- The entity must attach evidence of publishing specific Public Datasets, under the FOI Regulations. - Responding to FOI requests can sometimes lead to the publication of open datasets as part of the Open Data (OD) initiatives. - When a requestor submits an FOI request to obtain specific information that is within the scope of FOI Regulations, and the request is granted, the government entity may provide the requested information in the form of a dataset. If a published dataset meets the criteria of being publicly available, machine-readable, and reusable, it can be considered Open Data (OD).
	- Evidences of the Published FOI Communications	- The entity must attach evidence of the FOI communication publications, including guidelines and Frequently Asked Questions (FAQs), on the entity's official website, in line with NDMO requirements.
	- The Pricing Scheme for Public Information Access Requests.	- The entity must attach a public information access request pricing mechanism. The entity must calculate and document the processing fees of each granted / approved public-information access request, by adopting a Pricing Scheme determined by the entity.
	- The Up-to-date FOI Register.	- The entity must attach an updated FOI Register as the entity must document compliance records in a register as instructed in the FOI guidelines published by NDMO-SDAIA. The Register must include the following, at a minimum: • Information on the current Open Data and Information Access Officer (ODIAO). • Public Information Access Request Records. • Public entity Publications. • Any other records, including the manner and format, as required by the FOI Regulations published by NDMO-SDAIA.
Level 4: Managed	- The Monitoring Report with Pre-defined KPIs for the Entity's Responses on FOI Requests.	- The entity must attach an updated report on monitoring FOI processes based on pre-defined and identified KPIs and indicator cards, approved by the entity's authority holder. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator.

Checklist – Freedom of Information Domain

FOI.MQ.2	Has the entity defined and implemented the required processes for Freedom of Information (FOI)?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The Continuous Improvement Report on the FOI Processes.	- The entity must attach a report on the updated FOI process(es) including the changes, with reference to revised copies of the documents which identify the steps and procedures for a particular FOI process or task including: - The review documents and the documented periodic results of the updated processes, with the changes. - The FOI Processes continuous improvement mechanisms.
	- The Automated Tool for FOI Requests.	- The entity must attach a report describing (name, version, etc.) the tool(s) used to automate the FOI request responding process. - A tool refers to a program or an application designed to simplify and automate the process of handling / processing FOI requests from submission to completion. Such a tool can enhance efficiency, accuracy, and transparency in managing FOI requests by automating various tasks, reducing manual efforts, and ensuring compliance with FOI Laws and Regulations.

8.2.13. Data Classification Domain

Checklist – Data Classification Domain		
DC.MQ.1	Has the entity established a plan for Data Classification (DC) as stipulated by the Data Management and personal Data protection (DM & PDP) standards?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents
Level 1: Establishing	- The Existing DC Practices.	- The entity must attach a report clarifying the current Data Classification Practices.
Level 2: Defined	- The Defined & Approved Data Classification Plan.	- A recent Data Classification plan, approved by the entity's authority holder must be attached, including the following, at a minimum: - The roadmap with the activities & milestones for the classification of entity's data. The activities shall incorporate what is needed to achieve this Domain's specifications, at a minimum. - The assignment of the required resources & budget to manage the classification of the entity's data.
Level 3: Activated	- The Data Classification Implementation Plan Status Report.	- The entity must attach a report of the implementation status of the Data Classification Plan, including the following, at a minimum: Initiatives and projects status: Identifying the status of each initiative or project (started, in progress, completed, or delayed), along with clarification of any delays or challenges. Progress percentages: Providing the progress percentages of activities and milestones in the plan and roadmap, with clear details on the actual activities that have been completed. Supporting evidence: Attaching proof of achieved progress/completion, such as reports, photos, documents, or meeting minutes that support the implementation status.
Level 4: Managed	- The Implementation Monitoring Report of the DC Plan & Activities with Pre-defined KPIs.	- The entity must attach an updated report, approved by the entity's authority holder, on monitoring the effectiveness of the Data Classification plan based on pre-defined and identified KPIs and indicator cards. - Each indicator card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation.

Checklist – Data Classification Domain		
DC.MQ.1	Has the entity established a plan for Data Classification (DC) as stipulated by the Data Management and personal Data protection (DM & PDP) standards?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- Data Classification Plan Review Report.	- The entity must attach a report showing that the entity identified, implemented, and monitored continuous improvement mechanisms for the Data Classification Plan based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: - Reviews conducted. - Results of each review. - Improvements implemented (with supporting documents).

Checklist – Data Classification Domain		
DC.MQ.2	Has the entity defined, identified and implemented the required Data Classification (DC) processes?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents

Checklist – Data Classification Domain		
DC.MQ.2	Has the entity defined, identified and implemented the required Data Classification (DC) processes?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 1: Establishing	- The Current List of Classified Datasets.	- The entity must attach the current classified datasets list.
Level 2: Defined	- Data Classification Policy.	- Attach a data classification policy, which should include at a minimum: • Policy name. • Release date. • Release number. • Document control (preparation, revision, approval) • Version history. • Terminology. • Objective. • Scope of work. • References. • Policy owner. • Policy statement including at a minimum: • The main principles of classification • Classification prioritization process and criteria • Classification levels • Classification controls • Steps required for classification: 1. Define data. 2. Appointing the classification officer. 3. Conduct an impact assessment. 4. Conduct an impact assessment for low-impact data. 5. Classification review. 6. Apply appropriate controls. 7. Roles and responsibilities

Checklist – Data Classification Domain		
DC.MQ.2	Has the entity defined, identified and implemented the required Data Classification (DC) processes?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Data Handling and Protection Controls.	- The entity must attach a document containing the Handling & Protection Controls for each Dataset & Artifact according to its classification, to ensure secure handling, processing, sharing and disposal of data by following the policies & regulations of the National Cybersecurity Authority (NCA). The document shall include, at a minimum: • The controls for protection, handling & processing of Public Classification cases. • The controls for protection, handling & processing of Confidential Classification cases. • The controls for protection, handling & processing of Confidential / Secret Classification cases. • The controls for protection, handling & processing of Top Confidential / Top Secret Classification cases.
Level 3: Activated	- The Inventory Report of the Identified Datasets and Artifacts.	- The entity must attach a document clarifying an inventory of all datasets & artifacts to implement the Data Classification Process, including at a minimum: • Identifying the ownership of the datasets & artifacts. • The list of all datasets & artifacts.
	- The Prioritized Datasets and Artifacts.	- The entity must attach a document showing the list of prioritized datasets & artifacts to be followed during classification.
	- The Impact Assessment Report.	- The entity must attach a report proving that the entity conducts probable impact assessments (e.g., Any potential damage) when disclosing specific data or when specific data was accessed in an unauthorized way. The Impact Assessment process should be implemented for all identified datasets & artifacts, including the following steps: • The identification of the potential categories impacted, amongst national interests, organizations, individuals and environment. • The selection of the potential damage impact level for each identified category amongst 'High', 'Medium', 'Low' and 'None / Insignificant'. • The assignment of Classification Levels to datasets & artifacts based on the selected impact level: • If the impact level was assessed as 'High', then datasets & artifacts shall be classified as Top Confidential / Top Secret. • If the impact level was assessed as 'Medium', then datasets & artifacts shall be classified as Confidential / Secret.

Checklist – Data Classification Domain		
DC.MQ.2	Has the entity defined, identified and implemented the required Data Classification (DC) processes?	
Levels	Acceptance Evidence	Acceptance Criteria
		- If the impact level was assessed as 'Low', then datasets & artifacts shall be classified as Confidential. - If the impact level was assessed as 'None / Insignificant', then datasets & artifacts shall be classified as Public. - The assessment alignment with the Data Classification Policies & Regulations published by NDMO-SDAIA.
	- The Assessment Report of Low-Impact Data.	- A report shall be attached proving that the entity researched / assessed the possibility of Classifying Low-impact data as Public instead of Confidential. The assessment shall include the following: - Analyzing / evaluating if the disclosure of this Low-impact data breaches any existing KSA regulation such as the Anti Cyber Crime Regulations and the Electronic Commerce (e-Commerce) Regulations. - Identifying the potential benefits of disclosing / opening such Datasets & Artifacts and assuring / considering whether those would outweigh the negative impacts. - Modifying the Low-impact classified data to be considered Public if publishing / releasing would not breach any applicable / existing regulation, especially if the benefits outweigh the negative impacts. - Aligning the assessment with the Data Classification Policies & Regulations published by NDMO-SDAIA.
	- Evidences of Utilization of the Data Catalog Tool for the Data Inventory.	- The entity must attach a report or a proof that the Data Catalog Tool was used for Data Inventorying.
	- The Approved Data Access List of users with the Assigned Privileges.	- The entity must attach a document showing the Data Access list with the assigned permissions / privileges, including the following, at a minimum: - Specifying the types of users who need Data Access. - Specifying the Data Access Authorizations (Read, Modify, Delete).

Checklist – Data Classification Domain		
DC.MQ.2	Has the entity defined, identified and implemented the required Data Classification (DC) processes?	
Levels	Acceptance Evidence	Acceptance Criteria
	- Data Register.	- The entity must attach a register / log documenting the list of all identified datasets & artifacts, in addition to the activities implemented during the Data Classification process. The register / log should include the following, at a minimum: • The list of the entity's identified datasets & artifacts. • The Classification Levels assigned to the identified datasets & artifacts. • The Assignment Dates of the classification levels to the identified datasets & artifacts. • The mandatory Classification Durations of the identified datasets & artifacts. • The Classification Levels approved / validated during the reviews. • The Classification Levels' Review Dates.
Level 4: Managed	- The Monitoring Report of the DC Processes with Pre-defined KPIs.	- The entity must attach an updated report, approved by the entity's authority holder, on monitoring the effectiveness of DC processes based on pre-defined and identified KPIs and indicator cards, covering: • The percentage of Classified datasets & artifacts (out of the entity's total datasets & artifacts). • The percentage of datasets & artifacts classified with specific classification levels (out of the entity's total Classified datasets & artifacts). • The percentage of Low-impact data classified as Confidential. • The percentage of Classified datasets & artifacts that were reviewed, approved & validated. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description.

Checklist – Data Classification Domain		
DC.MQ.2	Has the entity defined, identified and implemented the required Data Classification (DC) processes?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- The Data Classification Automation Tool.	- The entity must attach a report demonstrating the following, at a minimum: - A description of the solutions and tools used in the process of automating DC. - A description of the processes and stages involved in automating DC. - Samples of the tools used in the process of automating DC. - Samples of the data classified using DC automation tools.

Checklist – Data Classification Domain		
DC.MQ.3	Has the entity reviewed all its classified datasets and artifacts to ensure that the classification levels assigned to them are the most appropriate ones as specified by the Data Classification (DC) Policies?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0:	No required documents	No required documents

Checklist – Data Classification Domain		
DC.MQ.3	Has the entity reviewed all its classified datasets and artifacts to ensure that the classification levels assigned to them are the most appropriate ones as specified by the Data Classification (DC) Policies?	
Levels	Acceptance Evidence	Acceptance Criteria
Absence of Capabilities		
Level 1: Establishing	- The Current Practices of DC Reviews.	- The entity must attach a report clarifying the current practices of reviewing the classification of all Classified Datasets & Artifacts for the following: • To ensure that the assigned classification level for each is suitable based on the Data Classification Policies & Regulations. • To change the classification level if the data status changes.
Level 2: Defined	- The DC Review Mechanism.	- The entity must attach a document specifying the Data Classification Review Mechanism, as well as the roles and responsibilities related to all stages of the classification review process, in accordance with the Data Classification Policy. The document must include, at a minimum, the following: • Procedures for verifying the accuracy of the data collected. • Procedures for verifying data classification levels. • Procedures for verifying validity. • Procedures for Identifying errors and corrections. • Procedures for documenting the Data Classification Review Process.
Level 3: Activated	- The Data Classification Review Report.	- The entity must attach a report that proves periodic Data Classification reviews in accordance with the defined classification review mechanism and the Data Classification Policy issued by NDMO-SDAIA. The report must, at a minimum, include the following: • The Reviewed Classified datasets & artifacts. • The Decisions made resulting from the Review Process.
	- An Evidence Document of the Published Classification Levels as Metadata.	- The entity must attach a document proving that the entity published on the comprehensive Data Catalog the classification levels assigned to the datasets. The Metadata must be published according to the process defined in the Data Catalog & Metadata (MCM) Data Management (DM) Domain (i.e., Metadata & Catalog Management (MCM)).
Level 4: Managed	- The Monitoring Report of the DC Review Mechanism with Pre-defined KPIs.	- The entity must attach an updated report, approved by the entity's authority holder, on monitoring the effectiveness of the DC Review Mechanism based on pre-defined and identified KPIs and indicator cards. - Each indicator card must include the following, at a minimum: • Indicator's Name / Code. • Indicator's Owner. • Indicator's Coordinator. • Indicator's Description.

Checklist – Data Classification Domain

DC.MQ.3	Has the entity reviewed all its classified datasets and artifacts to ensure that the classification levels assigned to them are the most appropriate ones as specified by the Data Classification (DC) Policies?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- Data Classification Review Mechanisms Review Report.	- The entity must attach the continuous improvement report of DC Review based on the results of the KPI measurements and relevant updates and developments in the domain, containing the following, at a minimum: - Evidence of the automation of DC review processes and the automated application of the new classification to the Data Catalog tool. - Review and results documentation: Periodic review and result documentation for DC reviews. - Continuous improvement mechanisms: Mechanisms for the continuous improvement of DC reviews.

8.2.14. Personal Data Protection Domain

Checklist – Personal Data Protection Domain		
PDP.MQ.1	Has the entity performed an initial Personal Data Protection (PDP) assessment and developed a plan to address the strategic and operational Privacy requirements?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	No required documents	No required documents
Level 1: Establishing	- Evidences of the existing practices of the PDP Domain and Data Privacy.	- A report must be attached showing current PDP& data privacy practices, including proofs for those practices.
	- The Initial PDP Assessment Result.	- The assessment should be aligned with national Personal Data Protection Law (PDPL) and include the following, at a minimum: • Identification of the types of personal data being collected. • Location & method of personal data storage. • Current processing & uses of the personal data. • Privacy challenges in meeting compliance with PDPL rules and the executive regulations published by NDMO-SDAIA.
Level 2: Defined	- The Approved PDP implementation plan.	- The plan should include the following, at a minimum: • A roadmap of activities & milestones to achieve conformity commitment and maintain full compliance with the PDP Policies published by NDMO-SDAIA. The activities shall include what is necessary to achieve the PDP Domain specifications, at a minimum. • Allocating the required resources & budget to meet full compliance with PDPL rules and executive regulations.
	- The PDP Training plan.	- A report must be attached including an approved valid plan for training the entity's employees in the PDP Domain, including, at a minimum: • The scope & objectives of the training process including the various PDP Domain topics mentioned in the "Data Management and Personal Data Protection (DM & PDP) Standards" document. • The methods & channels through which the training plan will be implemented. • The training plan execution dates.
Level 3: Activated	- The PDP Plan Implementation Status Report.	- A report must be attached demonstrating PDP plan implementation status including, at a minimum: • Initiatives and projects status: Identifying the status of each initiative or project (started, in progress, completed, or delayed), along with clarification of any delays or challenges.

Checklist – Personal Data Protection Domain		
PDP.MQ.1	Has the entity performed an initial Personal Data Protection (PDP) assessment and developed a plan to address the strategic and operational Privacy requirements?	
Levels	Acceptance Evidence	Acceptance Criteria
		Progress percentages: Providing the progress percentages of activities and milestones in the plan and roadmap, with clear details on the actual activities that have been completed. Supporting evidence: Attaching proof of achieved progress/completion, such as reports, photos, documents, or meeting minutes that support the implementation status.
	Evidence of PDP training activities conducted.	- A report must be attached showing the implementation status of the PDP training for all employees including, at a minimum: - The details of the training conducted for the entity's employees. - The training targets audience. - The methods & channels for the training. - The number of the entity's employees who were trained in the PDP Domain, and a list of training topics including the following: - Importance of Personal Data Protection and the Impacts and consequences to the entity and / or Data Subject. - Definition of Personal Data. - Data Subject Data Rights. - entity and Data Subject Responsibilities. - Notifications as for when the entity and / or Data Subject should be notified and how to handle inquiries about personal data collection, processing and sharing.
Level 4: Managed	The Monitoring Report for the PDP Plan with pre-defined KPIs.	- The entity must attach an updated report, approved by the entity's authority holder on monitoring the effectiveness of the PDP plan based on pre-defined and identified KPIs and indicator cards. - Each indicator card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline. - Target value.

Checklist – Personal Data Protection Domain		
PDP.MQ.1	Has the entity performed an initial Personal Data Protection (PDP) assessment and developed a plan to address the strategic and operational Privacy requirements?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
Level 5: Pioneer	- Review Report and Continuous Improvement of the Personal Data Protection Plan.	- The entity must attach an updated report, approved by the entity's authority holder presenting continuous improvement of the PDP plan based on the results of the KPI measurements and relevant updates and developments in the domain containing the following, at a minimum: - Reviews conducted. - Results of each review. - Improvements implemented (with supporting documents).

Checklist – Personal Data Protection Domain		
PDP.MQ.2	Has the entity defined and implemented Privacy policies and processes for Personal Data including data breach identification, consent management, data subject rights, and Privacy risk assessments?	
Levels	Acceptance Evidence	Acceptance Criteria
Level 0: Absence of Capabilities	- No required documents	- No required documents
Level 1: Establishing	- Evidences of the existing initiatives for PDP and Data Privacy.	- Proofs must be attached for the current PDP & Data Privacy initiatives performed by the entity. For example, not limited to: - The entity's current PDP policies & processes. - Any documentation showing identified/monitored breach/leakage in personal data.

Checklist – Personal Data Protection Domain		
PDP.MQ.2	Has the entity defined and implemented Privacy policies and processes for Personal Data including data breach identification, consent management, data subject rights, and Privacy risk assessments?	
Levels	Acceptance Evidence	Acceptance Criteria
		- The documentation of the entity's current practices of consent management, and the rights of the Data Subjects. - Privacy risk assessments conducted by the entity.
Level 2: Defined	- The documented Data Breach Notifications Process.	- The entity must attach a document outlining the processes for data breach notifications. This document should specify that the person responsible for data control or data processing, who handles personal data at the entity, is required to notify the regulatory authority in the event of a personal data breach within the timeframe specified in the PDPL rules and the executive regulations issued by the National Data Management Office. Note that the timeframe for reporting is 72 hours. - Please refer to PDPL rules and executive regulations issued by NDMO-SDAIA for more detailed requirements.
	- The documented Data Breach Management Process.	- A document must be attached containing the procedures & processes of Data Breach Management. The Data Breach Handling Management Process shall include, at a minimum: - Conducting an incident review by the Data Controller / Data Protection Controller with the Regulatory Authority. - Formulating an immediate response to the incident by the Data Controller and/or Data Processor. - Implementing the permanent corrective actions as issued by the Regulatory Authority. - Testing the implemented corrective actions to validate the PDP solution(s) efficiency.
	- The PDP & Data Privacy Notice and the Consent Management Process.	- The entity shall attach a document containing the procedures & processes of the PDP / Privacy Notice and Consent Management Process considering the following components, at a minimum: - Define and document the processes of providing data subjects with notice and requesting consent at all the data lifecycle phases where/when data is collected based on PDPL rules and executive regulations issued by NDMO-SDAIA. - The entity shall provide the Data Subject with all possible options; and the entity must get the Data Subject's (Explicit or Implicit) consent / approval regarding the collection, use or disclosure of personal data. - The entity shall document and make available a PDP/Privacy Notice/Notification for data subjects to read/review before or at the time the entity requests permission to collect personal data.

Checklist – Personal Data Protection Domain		
PDP.MQ.2	Has the entity defined and implemented Privacy policies and processes for Personal Data including data breach identification, consent management, data subject rights, and Privacy risk assessments?	
Levels	Acceptance Evidence	Acceptance Criteria
	- The Data Subjects' Rights Management Processes.	- The entity shall attach the Data Subjects Rights Management Procedures & Processes document as it's a must to establish & document the operations to support the rights of data subjects, in compliance with PDPL rules and executive regulations issued by NDMO-SDAIA, whereby a data subject has the following rights: • Right to be informed. • Right to access. • Right to rectify / correct. • Right to erase or destroy. • Right to object. • Right to restrict processing. • Right to data portability / transfer. - The entity should inform the Data Subjects about their rights and provide possible means by which Data Subjects requests are submitted, responded to and tracked.
	- Entity-Specific PDP Policies.	- The entity shall attach its PDP Policies document approved by the authority holder, for the protection of its personal data. The policy must include the entity's commitment to the PDPL rules and its executive regulations issued by NDMO-SDAIA. - The policy must include: • Policy Name. • Release date. • Version number. • Document control (Preparation, review, approval). • Policy Statement. • Job roles & responsibilities. • Version history / record. • Terminologies. • Objective. • Scope of work. • References. • Policy Owner.
Level 3: Activated	- The Developed & Adopted Consent Management Workflow.	- Evidences shall be attached proving the automation of the developed & approved workflow for the consent management process.
	- Evidences of Notifications Sent to the Regulatory Authority within the Allotted Timeframe.	- Evidences shall be attached proving that the notifications were sent by the person in charge of data control or data processing who deals with personal data at the entity, to

Checklist – Personal Data Protection Domain		
PDP.MQ.2	Has the entity defined and implemented Privacy policies and processes for Personal Data including data breach identification, consent management, data subject rights, and Privacy risk assessments?	
Levels	Acceptance Evidence	Acceptance Criteria
		the regulatory/legislative authority within the specified reporting time frame of 72 hours. If no incident occurred, an approved letter should be attached.
	- Evidences of Data Breach Management Including Identified Data Breaches.	- Evidences shall be attached proving that data breach Management, including the identification & detection of data breaches which occurred. If no incident occurred, an approved letter should be attached.
	- The Results of the PDP Risk Assessments.	- The entity shall attach a document containing the procedures & processes of the PDP risk assessments plan / operations, as it's a must that the entity conducts an annual risk assessment of the operation and use of the information systems containing personal data, including the collection & processing of personal data, and the storage & transmission of personal data by each system whether automated or manual. The risk assessment findings must be as follows, at minimum: - Documented. - Analyzed for impact and the occurrence likelihood. - Evaluated against current regulations obligations and resolution criticality.
	- Evidences of Published Data Subjects Rights Management Processes and Feedback Received from Data Subjects.	- Evidences shall be attached proving that processes were published clearly, feedback was collected from users, especially Data Subjects.
	- The PDP Register.	- The entity should attach a report of the compliance records maintained (record of any collection or processing of any personal data), and evidence showing that the records were made available to the regulatory authority (NDMO) as defined in the PDPL rules and its executive regulations issued by NDMO-SDAIA.
Level 4: Managed	- The Monitoring Report for the PDP & Data Privacy Practices based on pre-identified KPIs	- The entity must attach an updated report, approved by the entity's authority holder, on monitoring the effectiveness of PDP processes based on pre-defined and identified KPIs and indicator cards. - Each indicator card must include the following, at a minimum: - Indicator's Name / Code. - Indicator's Owner. - Indicator's Coordinator. - Indicator's Description. - The strategic/operational objective to be measured (with identifying the Specification or the Process to which the indicator belongs). - Indicator's Equation. - Measurement Unit (Percentage, Number / Quantity, etc.). - Baseline.

Checklist – Personal Data Protection Domain		
PDP.MQ.2	Has the entity defined and implemented Privacy policies and processes for Personal Data including data breach identification, consent management, data subject rights, and Privacy risk assessments?	
Levels	Acceptance Evidence	Acceptance Criteria
		- Target value. - Measurement Periodicity (Monthly / Quarterly / Biannually / Annually). - Data sources used to calculate the indicator. - Data collection mechanism (manual/automated). - Indicator's polarity (+/-) (Positive Polarity: Higher indicator value is the target, Negative Polarity: Lower indicator value is the target). - The current indicator value compared to the target value. - Indicator status (achieved/delayed/not achieved, etc.). - The report should also include: - Recommendations to improve performance based on the actual indicator values. - Supporting documents for the data used to calculate the indicator values
	- The Compliance Monitoring Report & Audit Results.	- The entity shall conduct an internal audit to monitor compliance with the PDPL Rules & Data Privacy Regulations and shall document its findings in a report presented to the Data Protection Officer. In non-compliance cases, the entity shall take corrective actions and notify the Regulatory Authority and the NDMO and shall document the corrective actions within the audit findings report.
Level 5: Pioneer	- The Documented Periodic Reviews & Outcomes for the PDP & Data Privacy Practices.	- A report must be attached including updated PDP & Data Privacy processes & practices documents, showing the operations of reviewing the PDP & Data Privacy processes & procedures. The report shall include, at a minimum: Based on the identified matters / issues, such as risk re assessment, the entity must update the documents (Policies & Procedures for combating everything related to breaching Data Privacy) and must attach an evidence of such reviews.
	- Evidences of Automation & Change Management for PDP.	- The entity must address changes on the PDP processes & practices and must attach continuous improvement mechanisms to prove effective Change Management in relation to the required changes. - The entity must attach an evidence of process automation (An updated workflow, any system changes) to include these changes as part of the implementation.



8.3. Appendix III – Operational Excellence (OE)

The Operational Excellence (OE) component of the NDI utilizes information captured from various national data platforms (e.g.: ODP, DL, DMP, GSB, NDC, and RDM) to evaluate the entity's operational efficiency and effectiveness based on the practices currently applied in 6 Data Management (DM) domains (subject to increase). For the second round of NDI, each entity will be measured against these metrics: DSI.OE.02, OD.OE.01, MCM.OE.01, MCM.OE.02, MCM.OE.03, RMD.OE.01, DQ.OE.02, DO.OE.02, DO.OE.03.

Please refer to “The Operational Excellence (OE) Document” for further details.

8.3.1.Data Sharing and Interoperability

Operational Excellence Metrics		
Metric ID	Metrics	Platforms
- DSI.OE.01	- Attributes shared on the Government Service Bus but not produced by the entity.	- Government Service Bus (GSB) - National Data Catalog (NDC)
- DSI.OE.02	- The entity's systems are integrated with National Data Lake.	- National Data Lake (NDL)
- DSI.OE.03	- The time taken to process data-sharing agreements.	- Data Marketplace (DMP)

8.3.2. Open Data

Operational Excellence Metrics		
Metric ID	Metrics	Platforms
- OD.OE.01	- Datasets published in the Open Data Platform.	- Open Data Platform (ODP)
- OD.OE.02	- Delay/Lag in refreshing open datasets.	
- OD.OE.03	- Number of reported issues for the published datasets.	
- OD.OE.04	- Delay in resolving reported issues on published datasets.	

8.3.3. Data Catalog and Metadata (MCM)

Operational Excellence Metrics		
Metric ID	Metrics	Platforms
- MCM.OE.01	- The entity's systems catalogued in the National Data Catalog.	- National Data Catalog (NDC)
- MCM.OE.02	- Business attributes defined and linked in the National Data Catalog.	
- MCM.OE.03	- KPIs and reports defined in the National Data Catalog.	
- MCM.OE.04	- Percentage of business attributes linked to attribute class standards in the National Data Catalog.	
- MCM.OE.05	- Accuracy percentage of business attribute relationships in the National Data Catalog.	

8.3.4. Reference and Master Data Management

Operational Excellence Metrics		
Metric ID	Metrics	Platforms
- RMD.OE.01	- Reference entities published by the entity.	- Reference Data Management platform (RDP). - Government Service Bus (GSB).
- RMD.OE.02	- Time taken to publish new reference entities.	
- RMD.OE.03	- Time taken to fix reported issues in reference entities	

8.3.5.Data Quality

Operational Excellence Metrics		
Metric ID	Metrics	Platforms
- DQ.OE.01	- The entity's Data Quality Index in the Government Service Bus.	- Government Service Bus (GSB)
- DQ.OE.02	- The entity's Data Quality Index in National Data Lake.	- National Data Lake (NDL)

8.3.6. Data Operations

Operational Excellence Metrics		
Metric ID	Metrics	Platforms
- DO.OE.01	- Response time for the entity's services (APIs) connected to the Government Service Bus.	- Government Service Bus (GSB)
- DO.OE.02	- Service responses on the Government Service Bus.	
- DO.OE.03	- Response of automated integration solutions with the National Data Lake.	- National Data Lake (NDL)

