National Data Management Office

Data Management and Personal Data Protection Standards

Version 1.5

January 2021

Document Control

Version	Revision Date	Contributor	Modification
1.0	Aug 2020	NDMO	First Issue
1.1	Sep 2020	NDMO	Refinement of selected sections
1.2	Oct 2020	NDMO	Incorporated comments received from government entities
1.3	Dec 2020	NDMO	Incorporated comments received from government entities
1.4	Jun 2021	NDMO	Incorporated comments received from government entities
1.5	Jun 2021	NDMO	Incorporated comments received from government entities

Table of Contents

1. Definitions

For the purposes of the KSA Data Management and Personal Data Protection Standards, the following words and phrases, wherever mentioned herein, shall have meanings ascribed thereto, unless the context requires otherwise:

Terminology	Definition
Data Management	The process of developing and executing plans, policies, initiatives, and practices to enable entities to manage and govern their data and achieve the aspired value, with data considered an organizational asset
Automated Data Catalog Tool	A metadata management tool designed to automate key features of data catalog including scanning and inventorying data sources, organizing metadata, browsing metadata and enabling users' collaborations by metadata tagging, annotations and ratings.
Business Partners	Entities engaged in producing, managing, or overseeing government data
Charging Model	The collection of rules associated with the generation of revenue associated with data held by Public Entities.
Data	A collection of facts in a raw or unorganized form such as numbers, characters, images, video, voice recordings, or symbols
Data Classification Levels	The four (4) levels of data classification defined by the National Data Management Office.
Data Controller	Any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data and/or carries out processing directly or through a Data Processor.
Data Processor	Any natural or legal person, public authority, agency or other body which processes personal data on behalf of a Data Controller.
Data Product (Processed Data)	Data Products are the outputs resulting from transforming data for added value by performing additional data collection, enrichment, preparation, analysis, or presentation.

Terminology	Definition
Data Requestor	Any natural or legal person, public authority, agency or other body which requests access to data held by a Government or Public Entity.
Data Sharing Agreement	A written agreement between a Public Entity and any Data Requestor governing the use of any shared data.
Data Subject	Any citizen of Saudi Arabia, alive or deceased, who can be identified, directly or indirectly, by data in the custody of the Data Controller.
Government Data	Raw data or processed data that is received, produced or held by public entities, regardless of the source, form or nature.
Master Data Object	A data element that is essential to record a transaction or observation in a digital storage system to properly record an external event or state.
Personal Data	Any element of data, alone or in connection with other available data, that would enable the identification of a Saudi citizen.
Public Entities	Any independent governmental or public entity or affiliates thereof in the Kingdom of Saudi Arabia. Furthermore, any company runs, operates or maintains public utilities or national infrastructure, or renders public service related to management of these public utilities or national infrastructure shall be deemed as a public entity
Public Information	Data, which is not classified as Confidential or higher, that has been determined by the Entity as eligible for release to the general public.
Reference Data Object	Agreed upon standards for representing common data elements, e.g. Zip codes, Country codes, temperature systems (Celsius vs Fahrenheit).
Trusted Source	An upstream data source which has proven to be reliable by verification in the past.
Unprocessed Data	Data that has not been subject to processing and exchanged in raw format at any volume

2. Introduction

DAMA is a non-profit global association, dedicated to advancing the concepts and practices of data management. Established in 1980, DAMA currently has 70 chapters across 33 countries around the world, each with a goal to promote the understanding and practice of managing data as a key asset supporting public and private organizations. To fulfill their mission, DAMA published the International Guide to Data Management Body of Knowledge (DAMA DMBOK), in addition to certifications, conferences, and trainings. As such, DAMA has been selected as a key reference for the Kingdom's National Data Management Standards.

Moreover, nations around the world are harnessing the value of data as the new oil and unlocking its innovation and economic potential. The Kingdom of Saudi Arabia generates, collects, and stores vast amounts of data that has substantial potential to contribute to its economic growth and welfare of its people. To enable the achievement of its data value, the Kingdom has developed the Data Management and Personal Data Protection Standards to govern and control the practice of data and build an effective data driven organization across government entities.

The National Data Management Office (NDMO), as the national regulator of data in the Kingdom, developed the Data Management and Personal Data Protection Standards based on the National Data Management and Personal Data Protection Framework along with the required controls and specifications for implementing and governing effective data management practices across government entities. Through these standards, NDMO also aims to govern data management related efforts and initiatives across entities.

2.1. Overview

The National Data Management and Personal Data Protection Standards document covers 15 Data Management and Personal Data Protection domains. To support the development of the Data Management and Personal Data Protection standards, a set of international references, internal relevant policies and regulations, and guiding principles were defined. Government Entities must implement the standards, and compliance will be measured yearly to monitor progress and drive efforts towards a successful implementation.

3. Purpose and Scope

The National Data Management and Personal Data Protection Standards have been developed pursuant to the directive issued by the Saudi Authority for Data and Artificial Intelligence under Cabinet Resolution number (292) dating 27/04/1441H which directs the National Data Management Office to develop and implement policies, governance mechanisms, standards and controls for data and artificial intelligence and monitor compliance upon publication. The

standards are defined for 15 domains as per the Data Management and Personal Data Protection Framework and are intended to be adopted by all Public Entities within the Kingdom.

In addition to Public Entities, the scope of the National Data Management and Personal Data Protection Standards also extends to business partners handling government data. Such business partners are responsible to understand and apply the Data Management and Personal Data Protection standards to all government data assets within their control and custody. The Standards apply to all government data regardless of form or type including paper records, emails, data stored in electronic form, voice recordings, videos, maps, photos, scripts, handwritten documents, or any other form of recorded data.

4. Compliance and Enforcement

The compliance assessment aims to measure the implementation of the National Data Management and Personal Data Protection Standards by Government Entities based on a defined compliance assessment methodology. Entities will conduct a compliance audit on an annual basis and submit the report to NDMO during the third quarter of each year. NDMO will review and consolidate all entity reports and publish to related stakeholders the annual compliance results at the entity, sector, and whole-of-government level.

Entities will conduct the compliance assessment at the level of each specification, with a binary value of either 100% assigned to specifications that are fully implemented, or 0% assigned to specifications that are partially or not implemented. The compliance score of each specification will be cascaded up to the control, domain, and overall Entity level. The annual compliance report shall also be supported with evidence for implementation of each specification where applicable. The compliance exercise shall be led by the Chief Data Officer, supported by the other Data Management and Personal Data Protection Office roles.

Based on the outcomes of the submitted Entity Compliance Reports, NDMO may conduct ad-hoc Compliance Audits on selected entities to further review and validate findings.

5. Data Management Guiding Principles

The National Data Management Office has defined Data Management Guiding Principles anchoring the development of the National Data Management and Personal Data Protection Standards. These principles assist in the understanding of the overall Data Management and Personal Data Protection landscape which map to the 15 domains as stated in the table below.

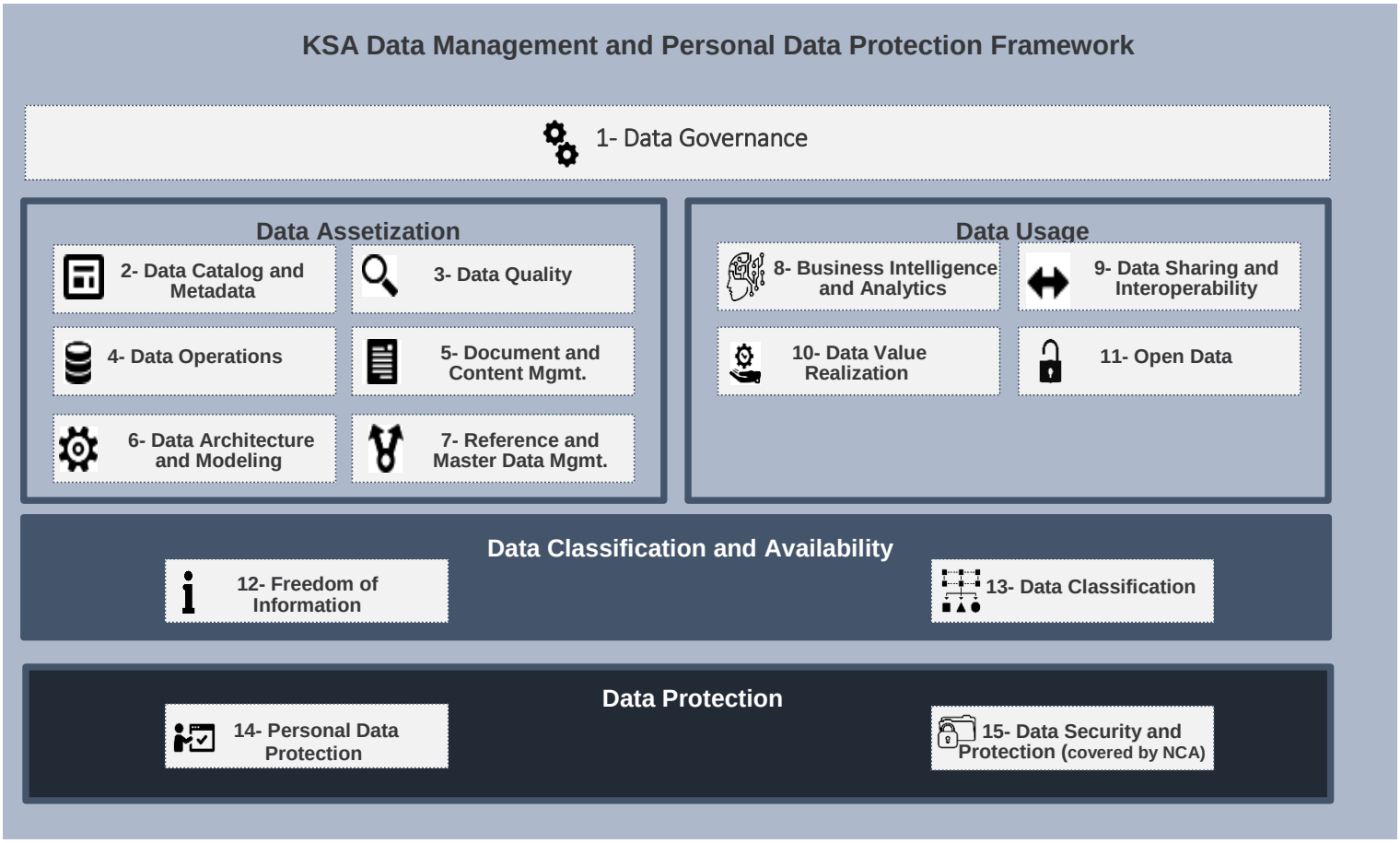
Principle	Definition	Mapped Domain(s)
Data as a National Asset	As any public sector asset, Government data should be discoverable, protected and	• Data Governance

Principle	Definition	Mapped Domain(s)
	maintained with clear accountability and with the potential to be monetized.	
Data Protection by Design	Build systems and processes that are proactive in protecting the privacy of individuals as well as their right to consent and/or refuse under the applicable KSA laws.	• Personal Data Protection • Data Classification • Data Security and Protection
Open by Default	Ensure that the Government avail most of its data to the public by default unless there is sufficient justification that non-disclosure of data is of greater public interest.	• Open Data
Ethical Data Use	Build ethical practices and norms around the governance and usage of data with fairness, traceability and contribution to the "Common Good" at the heart of these practices in alignment with the tenants of the Saudi culture.	• Data Governance
Purposeful Design	Adopt a human-centric and responsive approach for data collection, processing, sharing, and usage to meet the future needs of the Kingdom.	• Data Operations • Data Sharing and Interoperability • Data Architecture • Reference and Master Data Management
Data-Driven Outcomes	Build the next Generation Public Sector where most of the operational and strategic decisions as well as policy formulation are based on data insights.	• Business Intelligence and Analytics • Data Value Realization
Learning Culture	With the anticipated accelerating technology advancements in Data Management and the competitive market landscape, ensure that Saudi talent and human capital is continuously learning, adapting, and leading regionally.	• Data Value Realization • Business Intelligence and Analytics • Data Governance
Trusted Data	Build trust among the Government and with the Public either through ensuring high quality data or by being transparent about the level of quality	• Data Quality • Reference and Master Data Management • Data Catalog and Metadata • Document and Content Management

6. KSA Data Management and Personal Data Protection Framework

The standards including the controls and specifications have been defined across 15 Domains presented in the KSA Data Management and Personal Data Protection Framework that span the data lifecycle from creation, storage, movement, usage, till retirement (see Figure 1).

Figure 1: KSA Data Management and Personal Data Protection Framework



1. **Data Governance:** Data Governance provides the authority and control over the planning and implementation of the organization's data management practices through people, processes and technologies to provide consistent and proper handling of the organization's data assets in alignment to its Data Management and Personal Data Protection Strategy.

2. **Data Catalog and Metadata:** Data Catalog and Metadata focuses on enabling an effective access to high quality integrated metadata. The access to metadata is supported by use of the Data Catalog automated tool acting as the single point of reference to the organizations' metadata.

3. **Data Quality:** Data Quality focuses on the improvement of the quality of the organization data, ensuring that data is fit for purpose based on consumers' requirements.

4. **Data Operations:** The Data Operations domain focuses on the design, implementation, and support for data storage to maximize data value throughout its lifecycle from creation/acquisition to disposal.

5. **Document and Content Management:** Document and Content Management involves controlling the capture, storage, access, and use of documents and content stored outside of relational databases.

6. **Data Architecture and Modelling:** Data Architecture and Modelling focuses on establishment of formal data structures and data flow channels to enable end to end data processing across and within entities.

7. **Reference and Master Data Management:** Reference and Master Data Management allow to link all critical data to a single master file, providing a common point of reference for all critical data.

8. **Business Intelligence and Analytics:** Business Intelligence and Analytics focuses on analysing organization's data records to extract insight and to draw conclusions about the information uncovered.

9. **Data Sharing and Interoperability:** Data Sharing and Interoperability involves the collection of data from different sources and consists of integration solutions fostering a harmonious internal and external communication between various IT components. Data Sharing and Interoperability also covers a Data Sharing process that enable an organized and standardized exchange of data between entities.

10. **Data Value Realization:** Data Value Realization involves the continuous evaluation of data assets for potential data driven use cases that generate revenue or reduce operating costs for the organization.

11. **Open Data:** Open Data focuses on the organization’s data which could be made available for public consumption to enhance transparency, accelerate innovation, and foster economic growth.

12. **Freedom of Information:** Freedom of Information domain focuses on providing Saudi citizens access to government information, portraying the process for accessing such information, and the appeal mechanism in the event of a dispute.

13. **Data Classification:** Data Classification involves the categorization of data so that it may be used and protected efficiently. Data Classification levels are assigned following an impact assessment determining the potential damages caused by the mishandling of data or unauthorized access to data.

14. **Personal Data Protection:** Personal Data Protection focuses on protection of a subject's entitlement to the proper handling and non-disclosure of their personal information.

15. **Data Security and Protection:** Data Security and Protection focuses on the processes, people, and technology designed to protect the entity's data, including, but not limited to authorized access to data, avoidance of spoliation, and safeguarding against unauthorized disclosure of data. This domain is under the mandate of the Saudi National Cybersecurity Authority.

7. Control Structure

The standards control structure adopted follows a 3-level hierarchy:

1. Domain level – the domain is a knowledge area defined by the KSA Data Management & Privacy Framework
2. Control level – the control is a grouping of the specifications addressing a common area within the domain
3. Specification level – the specification defines the required outcomes that need to be realized to be compliant with the Data Management & Privacy Standards

As such, each of the 15 Data Management & Privacy domains breaks down to a set of controls that further break down into a list of related specifications.

- For each control area, the control description, ID, and dependencies are defined
- For each specification, the specification #, description and priority level are defined

Figure2: Control Structure Format

Domain Name	Name of the Domain	**Domain ID**	#
Control Name	Name of the Control	**Control ID**	#
Control Description	Description of the Control		

Specification #	**Specification Name**	**Control Specification**	**Priority**
Specification ID#	Specification Name	Description of the Specification	Priority #

Version History	
Date	**Version**
Dependencies	Control Dependencies

ID	Element name	Description
1	**Domain Name**	A name of the Domain, e.g. Data Governance
2	**Domain ID**	A unique identifier of the Domain, e.g. DG for Data Governance
3	**Control Name**	A name of the Control. e.g. Policy and Guidelines
4	**Control ID**	A unique identifier of the Control using the following format [DomainID.NUMBER] where NUMBER is ordering number of the Control within the Domain An example: DG.2 is a second control within Data Governance domain
5	**Control Description**	A high-level description of the Control including the Specifications covered
6	**Specification #**	A unique identifier of the Specification using the following format [Control ID.NUMBER] where NUMBER is ordering number of the Specification within the Control An example: DG.2.2 is the second Specification within the second Control within Data Governance domain
7	**Control Specification**	The activities / tasks required in order to achieve compliance
8	**Priority**	A priority determining the order in which the Control's Specifications shall be addressed
9	**Version History**	The version history allowing versioning control of changes following release of the document.
10	**Dependencies**	Pre-requisite for other Controls the Entity must be complied with to ensure that this Control is effective

8. Specifications Prioritization

The KSA National Data Management and Personal Data Protection Standards Specifications are assigned with priorities reflecting the required order for implementation.

8.1. Prioritization Details

The KSA National Data Management and Personal Data Protection standards includes 77 controls and 191 specifications. The specifications have been prioritized as follows:

- **Priority 1 (P1)**: Required specifications that must first be implemented as foundational building blocks in developing data management capabilities. These shall be implemented by all adopting entities in the first year from the release of these standards.
- **Priority 2 (P2)**: Required specifications that should be implemented to improve data management capabilities. These shall be implemented by all related entities from the second year of the release of these standards.
- **Priority 3 (P3)**: Required specifications that should be implemented to further advance the maturity of data management capabilities. These shall be implemented by all related entities from the third year of the release of these standards.

Summarized below, the span of controls and specifications across 15 domains:

ID	Domain	# of Controls	# of Specifications	Specifications Priority		
				P1	P2	P3
1	**Data Governance**	8	28	18	9	1
2	**Data Catalog and Metadata**	6	20	5	13	2
3	**Data Quality**	4	13	3	8	2
4	**Data Operations**	5	14	3	10	1
5	**Document and Content Management**	5	12	5	4	3
6	**Data Architecture and Modelling**	7	13	3	10	0
7	**Reference and Master Data Management**	6	18	8	10	0
8	**Business Intelligence and Analytics**	5	10	4	5	1
9	**Data Sharing and Interoperability**	8	16	8	7	1

10	**Data Value Realization**	4	8	2	5	1
11	**Open Data**	5	10	4	5	1
12	**Freedom of Information**	4	9	4	3	2
13	**Data Classification**	5	10	5	4	0
14	**Personal Data Protection**	5	10	4	5	1
15	**Data Security and Protection**	*The controls and specifications for this domain shall be addressed by the National Cybersecurity Authority (NCA)*				
--	**Total**	**77**	**191**	**76**	**98**	**16**

8.2. Implementation Plan

The specifications' priorities shall be treated as an input for the development of a phased implementation plan ensuring the Entity's compliance with KSA Data Management and Personal Data Protection Standards. The plan shall be based on a three-year roadmap for implementing all required specifications. The implementation plan shall include three main milestones:

1. The end of Year 1 – all specifications with Priority 1 (P1) are implemented
2. The end of Year 2 – all specifications with Priority 1 and 2 (P1 and P2) are implemented
3. The end of Year 3 – all specifications with Priority 1, 2 and 3 (P1, P2 and P3) are implemented

As such, the Entity's compliance to the standards will cover in year 1 Priority 1 specifications only, in year 2 Priority 1 and 2 specifications only, and in year 3 Priority 1, 2 and 3 specifications

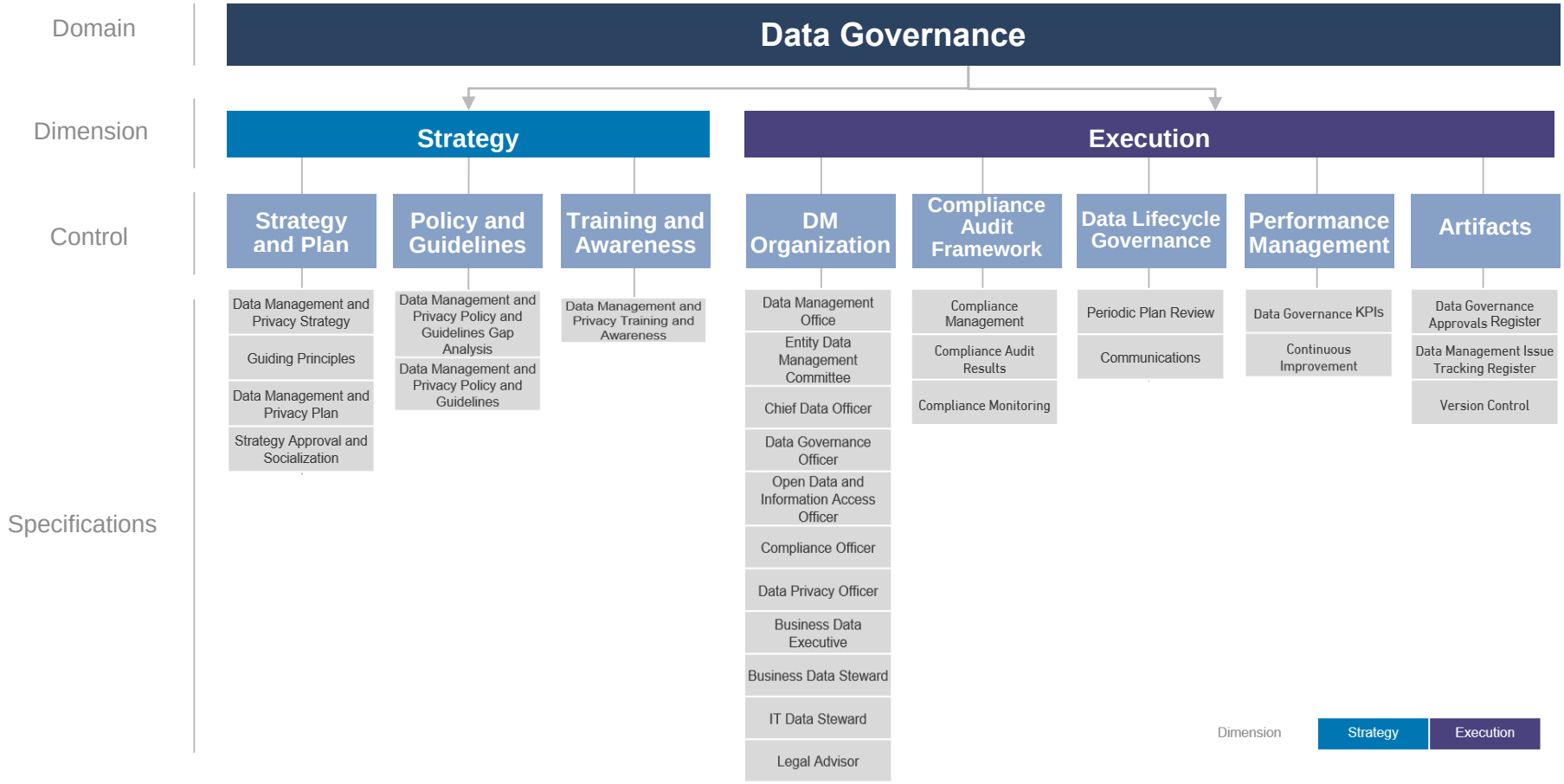
9. KSA Data Management and Personal Data Protection Standards

In this section, the specific controls and specifications identified are listed based on the previously introduced structure and segmented into 3 priority levels. These will be presented per domain, for each of the 15 domains of the KSA Data Management and Personal Data Protection Framework

9.1. Data Governance Domain

9.1.1. Domain on a Page

Data Governance domain comprises of 8 controls and 28 specifications. This domain provides the authority and control over the planning and implementation of the organization's data management practices



9.1.2. Controls and Specifications

Domain Name	Data Governance	Domain ID	DG

Control Name	Strategy and Plan	Control ID	DG.1
Control Description	As part of the Strategy and Plan control, the Entity shall establish a Data Management and Personal Data Protection Strategy and develop a Data Management and Personal Data Protection Plan		

Specification #	Specification Name	Control Specification	Priority
DG.1.1	Data Management and Personal Data Protection Strategy	The Entity shall establish a Data Management and Personal Data Protection Strategy to align Entity data initiatives and relevant stakeholders to achieving its business goals, in alignment with the overall program strategy. The Strategy shall cover all domains and reflect: 1. Current data management challenges 2. Strategic requirements covering internal requirements derived from the Entity's business strategy as well as external requirements derived from the National Data Management Agenda 3. Data Management and Personal Data Protection Vision, Mission and Strategic Goals and Objectives 4. Strategic and Operational performance metrics with targets across the 3 to 5 years strategy duration 5. Required financial budget for the implementation of the strategy, broken down by initiatives.	P1

DG.1.2	**Guiding Principles**	The Entity shall adopt the National Data Management and Personal Data Protection Program's Guiding Principles to affirm alignment of the Entity's Data Management and Personal Data Protection Strategy to the National Data Management and Personal Data Protection agendas. The Entity may, at its discretion, include additional Entity-level guiding principles to augment the core set of NDMO Guiding Principles. Adoption of the National Data Management and Personal Data Protection Program's Guiding Principles shall be articulated either in the Data Management and Personal Data Protection Strategy or as a standalone document. The guiding principles establish a data-centric culture where all stakeholders are unified in understanding what is most important for the Entity's Data Management and Personal Data Protection agendas.	P1
DG.1.3	**Data Management and Personal Data Protection Plan**	Based on the Entity's defined Data Management and Personal Data Protection Strategy, the Entity shall develop a Data Management and Personal Data Protection Plan with a 3-year implementation roadmap. The implementation roadmap shall include, at minimum, the following: 1. Initiatives that cover all the Data Management Domains defined in these standards and in alignment with the National Data Management and Personal Data Protection Framework 2. Prioritization of the list of initiatives based on a prioritization framework such as, at minimum, Impact versus Ease of Implementation 1. Highlight of the initiatives that are Quick Wins and planned to be implemented within the first 6 months, and the mid to long term initiatives that are planned throughout the 3-year period.	P1

DG 1.4	**Strategy Approval and Socialization**	The Entity shall obtain formal approval of their Data Management and Personal Data Protection Strategy by the Entity's Data Management Committee and other related senior level executives within the Entity. The Entity shall also socialize and raise awareness of the Data Management and Personal Data Protection Strategy in one or more internal workshops.	P1

Version History	
June 2020	**Version 1.0**

Dependencies	- **None**

Domain Name	Data Governance	Domain ID	DG

Control Name	Policy and Guidelines	Control ID	DG.2
Control Description	As part of the Policy and Guidelines control, the Entity shall conduct a Data Management and Personal Data Protection Policy and Guidelines gap analysis, and develop the Entity specific Data Management and Personal Data Protection Policy and Guidelines		

Specification #	Specification Name	Control Specification	Priority
DG.2.1	Data Management and Personal Data Protection Policy and Guidelines Gap Analysis	To support implementation of the Entity's Data Management and Personal Data Protection Strategy, the Entity shall conduct a Data Management and Personal Data Protection Policy and Guidelines gap analysis, including, at minimum, the following: 1. An analysis of the National Data Management and Personal Data Protection Program's Policies, Standards, and Guidelines 2. Identification and analysis of all data related standards and policies currently published by the Entity or the Regulator of the sector to which the Entity belongs to 3. An analysis of the internal Entity-specific requirements for Data Management and Personal Data Protection Policies and Guidelines 4. A Data Management and Personal Data Protection Policies and Guidelines development plan that clearly indicates the timeline for implementation.	P1
DG.2.2	Data Management and Personal Data Protection Policy and Guidelines	The Entity shall develop the Entity specific Data Management and Personal Data Protection Policy and Guidelines, aligned to the National Data Management and Personal Data Protection Policies and Standards.	P1

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan**

Domain Name	Data Governance	Domain ID	DG

Control Name	Training and Awareness	Control ID	DG.3
Control Description	As part of the Training and Awareness control, the Entity shall conduct a Data Management and Personal Data Protection training to promote the agenda and enable a data-centric culture		

Specification #	Specification Name	Control Specification	Priority
DG.3.1	Data Management and Personal Data Protection Training	The Entity shall conduct Data Management and Personal Data Protection training for all related employees to promote the agenda and enable a data-centric culture. The training shall include, at minimum, the following: 1. Awareness of the national Data Management and Personal Data Protection laws, policies, and standards, and their applicability on the Entity 2. Awareness of the national Data Management and Personal Data Protection programs, and their applicability on the Entity 3. All 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.	P1

Version History	
June 2020	Version 1.0

Dependencies	- DG.1: Strategy and Plan - DG.4: Data Management and Personal Data Protection Organization

Domain Name	Data Governance	Domain ID	DG

Control Name	Data Management Organization	Control ID	DG.4
Control Description	As part of the Data Management Organization control, the Entity shall establish a Data Management Office and a Data Management Committee, and identify and appoint the relevant Data Governance roles		

Specification #	Specification Name	Control Specification	Priority
DG.4.1	Data Management Office	The Entity shall establish a Data Management Office to manage the achievement of the national data management agendas at the Entity level. The office responsibilities shall be aligned with the responsibilities defined in the “Organizational Manual” published by NDMO.	P1
DG.4.2	Entity Data Management Committee	The Entity shall establish a Data Management Committee aimed to provide direction and oversight to the overall data management agenda at the Entity level. The committee responsibilities shall be aligned with the responsibilities defined in the “Organizational Manual” published by NDMO.	P1
DG.4.3	Chief Data Officer	The Entity shall identify and appoint a Chief Data Officer to lead the Data Management and Personal Data Protection agenda. The Chief Data Officer's (CDO) responsibilities shall be highlighted in a job description and aligned with the responsibilities defined in the “Organizational Manual” published by NDMO.	P1
DG.4.4	Data Governance Officer	The Entity shall identify and appoint Data Governance Officer to support the data management agenda. The Data Governance Officer's responsibilities shall be highlighted in a job description and aligned with the responsibilities defined in the “Organizational Manual” published by NDMO.	P1
DG.4.5	Open Data and Information	The Entity shall identify and appoint an Open Data and Information Access Officer (ODIA) to support the data management agenda. The Open Data and Information Access Officer's responsibilities	P1

	Access Officer	shall be highlighted in a job description and aligned with the responsibilities defined in the “Organizational Manual” published by NDMO.	
DG.4.6	**Compliance Officer**	The Entity shall identify and appoint a Compliance Officer to audit and monitor the data management agenda. The Compliance Officer’s responsibilities shall be highlighted in a job description and aligned with the National Data Management Office’s with the responsibilities defined in the “Organizational Manual” published by NDMO.	P1
DG.4.7	**Personal Data Protection Officer**	The Entity shall identify and appoint a Personal Data Protection Officer (PDPO) to support the Personal Data Protection agenda. The Personal Data Protection Officer's responsibilities shall be highlighted in a job description and aligned with the responsibilities defined in the “Organizational Manual” published by NDMO.	P1
DG.4.8	**Business Data Executive**	The Entity shall identify and appoint Business Data Executives (BDE) to enable the data management agenda for their related domains. The Business Data Executive's responsibilities shall be highlighted in a job description and aligned with the responsibilities defined in the “Organizational Manual” published by NDMO.	P1
DG.4.9	**Business Data Steward**	The Entity shall identify and appoint Business Data Stewards to enable the data management agenda for their related domains. The Business Data Steward responsibilities shall be highlighted in a job description and aligned with the responsibilities defined in the “Organizational Manual” published by NDMO.	P1
DG.4.10	**IT Data Steward**	The Entity shall identify and appoint IT Data Stewards to enable the data management agenda from an IT perspective. The IT Data Steward responsibilities shall be highlighted in a job description and aligned with the responsibilities defined in the “Organizational Manual” published by NDMO.	P1

DG.4.11	**Legal Advisor**	The Entity shall identify and appoint a Legal Advisor to support in data related regulatory matters. The Legal Advisor's responsibilities shall be highlighted in a job description and aligned with the responsibilities defined in the "Organizational Manual" published by NDMO.	P1

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan**

Domain Name	Data Governance	Domain ID	DG

Control Name	Compliance Audit Framework	Control ID	DG.5
Control Description	As part of the Compliance Audit Framework control, the Entity shall establish Data Management and Personal Data Protection Compliance Management practices and document audit results and findings		

Specification #	Specification Name	Control Specification	Priority
DG.5.1	Compliance Management	The Entity shall establish Data Management and Personal Data Protection Compliance Management practices, and shall accordingly define the following: 1. Scope of the periodic compliance audit exercise 2. Processes to plan for and execute the compliance audits 3. Processes and tools to report compliance audit findings 4. Processes and plans for the remediation and escalation of non-compliance The processes shall be aligned to the National Data Management and Personal Data Protection Compliance Framework.	P2
DG.5.2	Compliance Audit Results	The Entity shall document results and findings from every compliance audit performed included in an Audit Report. The Audit Report(s) shall have, but not limited to, the following: 1. Compliance or non-compliance to each specification in this document 2. Clearly articulated findings with supporting evidence for each specification 3. Recommendations to remediate each instance of non-compliance 4. Accountable stakeholder for each recommendation, and the target date to complete the recommendation.	P2
DG.5.3	Compliance Monitoring	The Entity shall generate and monitor compliance audit scores by conducting periodic	P2

		compliance audits aligned to the national data management compliance framework, and to the Entity's defined processes for executing, reporting, remediating and escalating audit findings.	

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan** - **DG.2: Policy and Guidelines**

Domain Name	Data Governance	Domain ID	DG

Control Name	Data Lifecycle Governance	Control ID	DG.6
Control Description	As part of the Data Lifecycle Governance control, the Entity shall conduct periodic reviews for the Data Management and Personal Data Protection Plan and implement a communications capability to communicate updates on Data Management and Personal Data Protection activities and its effectiveness		

Specification #	Specification Name	Control Specification	Priority
DG.6.1	**Periodic Plan Review**	The Entity shall conduct periodic reviews to the Entity's Data Management and Personal Data Protection Plan, and document the outcome of these reviews, to ensure the plan maintains alignment towards the stated program objectives and evolving priorities. The Entity shall also document any changes to the initial approved plan where applicable.	P2
DG.6.2	**Communications**	The Entity shall implement a communications capability to communicate updates on Data Management and Personal Data Protection activities and its effectiveness. Communication updates shall be ongoing and, at minimum, include: 1. Key Data Management and Personal Data Protection program plan, activities and decisions 2. Storage of data management documents and artifacts 3. Measure of the data management performance metrics 4. Updates on the data management policies and processes 5. Updates on the compliance scores, compliance report, relevant regulatory environment and implementation plans.	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan** - **DG.5: Compliance Audit Framework**

Domain Name	Data Governance	Domain ID	DG

Control Name	Performance Management	Control ID	DG.7
Control Description	As part of the Performance Management control, the Entity shall establish key performance indicators (KPIs) to gather statistics on Data Governance and define, implement and monitor continuous improvement mechanisms for all Data Management domains		

Specification #	Specification Name	Control Specification	Priority
DG.7.1	**Data Governance KPIs**	The Entity shall establish key performance indicators (KPIs) to gather statistics on Data Governance. KPIs shall include, at minimum, the following: 1. Assignment of the Data Management and Personal Data Protection roles 2. Periodic Data Management and Personal Data Protection Committee Meetings completed 3. Development / Refresh of the Entity Specific Data Management Strategy and Policies 4. Trainings and awareness sessions completed 5. Participation in Training and Awareness Sessions 6. Compliance Audit Score 7. Start to finish cycle time to resolve data related issues reported to the Data Office 8. Number of change requests resolved and closed.	P2
DG.7.2	**Continuous Improvement**	The Entity shall define, implement, and monitor continuous improvement mechanisms for all Data Management domains. Improvements defined should relate to dimensions including the data organization and roles, processes, and technologies.	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan**

	- **DG.4: Data Management and Personal Data Protection Organization**

Domain Name	**Data Governance**	**Domain ID**	**DG**

Control Name	Artifacts	**Control ID**	**DG.8**
Control Description	As part of the Artifacts control, the Entity shall document in a register all data governance decisions, tracking logs and implement a version control for data management documents and artifacts		

Specification #	Specification Name	Control Specification	Priority
DG.8.1	**Data Governance Approvals Register**	The Entity shall document in a register CDO's approved data governance decisions along with their respective justifications.	P2
DG.8.2	**Data Management Issue Tracking Register**	The Entity shall document in a register historical records of data management related issues and resolutions raised by business and technical users.	P3
DG.8.3	**Version Control**	The Entity shall define and implement version control for data management documents and artifacts that the Entity is the creator of.	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan** - **DG.4: Data Management and Personal Data Protection Organization**

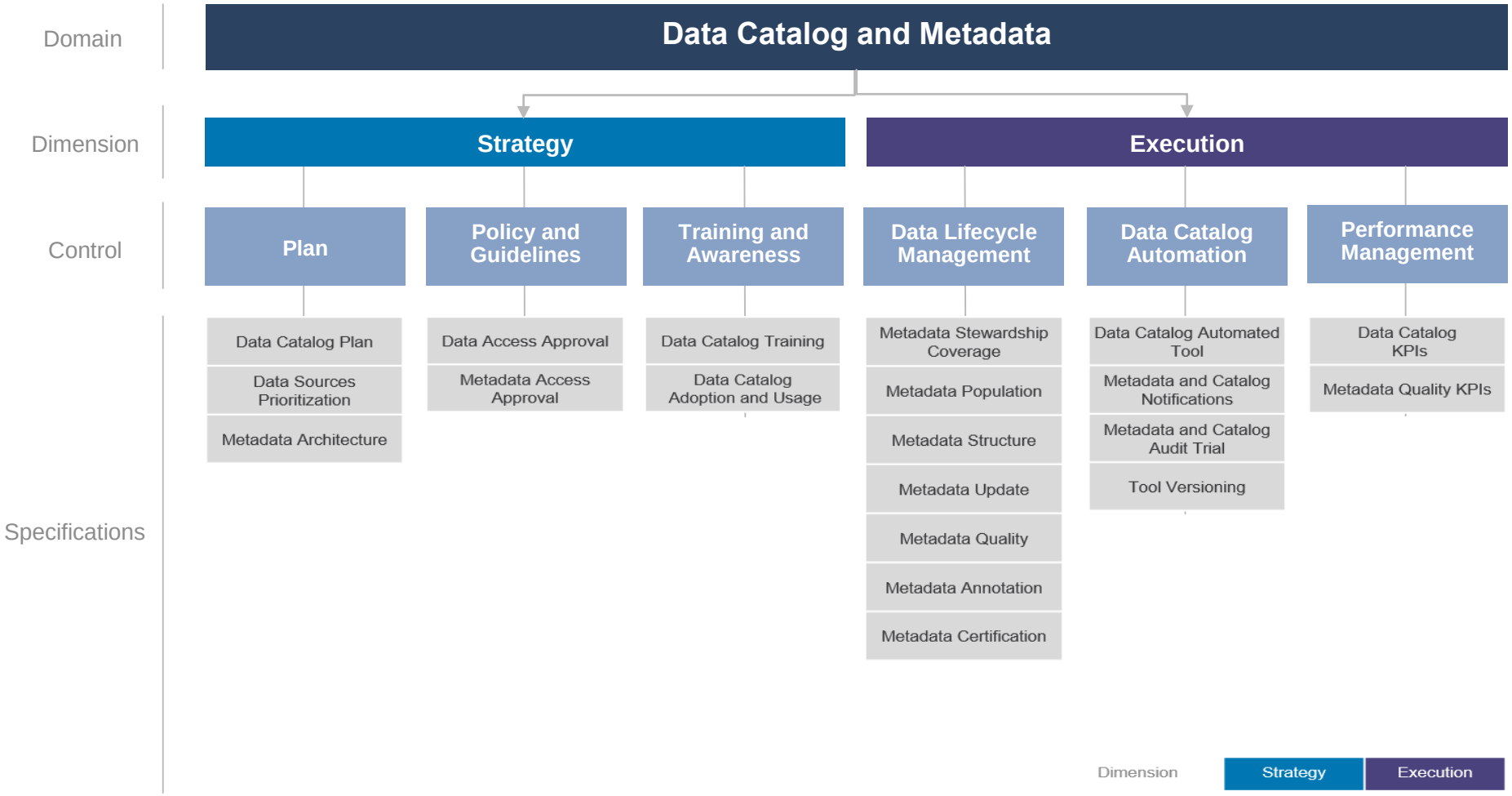
9.1.3. References

Data Governance Domain References	- DAMA DMBOK 2nd Edition (Mosley and Brackett, 2017) - Modern Data Strategy (Fleckenstein and Mike, 2019) - Data Governance (Ladley and John, 2012) - Building a Comprehensive Data Governance Program (Gartner, 2019) - Data Strategy (Marr and Bernard, 2017) - Accenture Data Governance Framework (Accenture, 2019)

9.2. Data Catalog and Metadata Domain

9.2.1. Domain on a Page

Data Catalog and Metadata domain comprises of 6 controls and 20 specifications. This domain focuses on enabling an effective access to high quality integrated metadata. The access to metadata is supported by use of the Data Catalog automated tool acting as the single point of reference to the organizations' metadata.



9.2.2. Controls and Specifications

Domain Name	Data Catalog and Metadata	Domain ID	MCM

Control Name	Plan	Control ID	MCM.1
Control Description	As part of the Plan control, the Entity shall develop a Data Catalog Plan and the target metadata architecture		

Specification #	Specification Name	Control Specification	Priority
MCM.1.1	Data Catalog Plan	Based on the Entity's defined Data Management and Personal Data Protection Strategy and Plan, the Entity shall create a Data Catalog Plan to manage the implementation of the Entity's Data Catalog. The plan shall include, at minimum, the following: 1. Roadmap with the activities and key milestones for the implementation of the Data Catalog automated tool. The activities shall, at minimum, incorporate what is needed to achieve the specifications in this domain 2. Assignment of the required resources and budget to manage the implementation of the Data Catalog automated tool.	P1
MCM.1.2	Data Sources Prioritization	The Entity shall prioritize data sources to be included in the Data Catalog, along with the definition of their business and technical metadata (or metadata structure)..	P1

MCM.1.3	**Metadata Architecture**	The Entity shall develop and document a target metadata architecture. The target metadata architecture shall include (but not limited to), the following: 1. Metadata sources - the Entity's data sources that are sources of metadata for the Data Catalog 2. Metadata repository - the Data Catalog as the Entity's central metadata repository 3. Metadata flows - a definition of metadata flows between the metadata sources and the metadata repository 4. Metadata model - a metadata model used by the Entity's Data Catalog.	P1

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan**

Domain Name	Data Catalog and Metadata	Domain ID	MCM

Control Name	Policy and Guidelines	Control ID	MCM.2
Control Description	As part of the Policy and Guidelines control, the Entity shall establish and follow clear processes for an approval of connecting the Data Catalog to the Entity's data sources and for providing the Entity's employees an access to the Data Catalog		

Specification #	Specification Name	Control Specification	Priority
MCM.2.1	Data Access Approval	The Entity shall establish and follow a clear process for the approval of connecting the Data Catalog tool to the Entity's Data Sources.	P2
MCM.2.2	Metadata Access Approval	The Entity shall establish and follow a clear process for providing the Entity's employees an access to the Data Catalog automated tool. The process shall implement role-based access to the Data Catalog, which includes the creation of access groups (for example read only, read and update, and administrator) and an assignment of the Data Catalog's users to these groups. The Data Catalog access groups shall be defined based on access rights to the Metadata and scope of the Metadata.	P2

Version History	
June 2020	Version 1.0

Dependencies	- DG.1: Strategy and Plan

Domain Name	Data Catalog and Metadata	Domain ID	MCM

Control Name	Training and Awareness	Control ID	MCM.3
Control Description	As part of the Training and Awareness control, the Entity shall conduct the Data Catalog trainings, accelerate adoption and increase usage of its Data Catalog		

Specification #	Specification Name	Control Specification	Priority
MCM.3.1	Data Catalog Training	The Entity shall conduct the Data Catalog training for every employee having direct need to discover, analyze or administer Metadata to promote the proper use of the Data Catalog. The training shall include, at minimum, the following: 1. Introduction of the Data Catalog concept and its benefits 2. Introductory and advanced tutorials about the Data Catalog automated tool and its functionalities 3. Hands-on exercises of the Data Catalog automated tool based on practical use cases.	P2
MCM.3.2	Data Catalog Adoption and Usage	The Entity shall push for an adoption and increase usage of its Data Catalog by: 1. Identification of Data Catalog power users - the Entity's Data Catalog advanced users that can act as coaches for other users 2. Creation of a communication plan announcing current Data Catalog power users and encouraging other Data Catalog users to interact with them. The plan shall include, at minimum, the following: 2a. Description of communication actions 2b. Frequency of communication actions 2c. Target audience.	P3

Version History	
June 2020	Version 1.0

Dependencies	- MCM.1: Plan

Domain Name	Data Catalog and Metadata	Domain ID	MCM

Control Name	Data Lifecycle Management	Control ID	MCM.4
Control Description	As part of the Data Lifecycle Management control, the Entity shall develop the Metadata structure and establish and follow processes for populating the metadata and managing of metadata quality issues		

Specification #	Specification Name	Control Specification	Priority
MCM.4.1	Metadata Stewardship Coverage	The Entity shall assign Business and IT Data Stewards to all the Metadata registered within the Data Catalog. Data Stewards assigned to the Metadata shall be continuously updated and shall reflect the most current Data Stewards' assignments within the Entity.	P2
MCM.4.2	Metadata Population	The Entity shall establish and follow a clear process for registering and populating the Metadata within the Data Catalog. The process shall be implemented as a workflow in the Data Catalog automated tool and by following the National Data Management Office's Data Catalog Guidelines.	P2
MCM.4.3	Metadata Structure	The Entity shall develop the Metadata structure according to the National Data Management Office's Data Catalog Guidelines. The Metadata structure defines Business Metadata attributes that are required to be populated in the Data Catalog. The Entity can augment the mandated Metadata structure with additional attributes based on the Entity's requirements.	P1
MCM.4.4	Metadata Update	The Entity shall establish and follow a clear process for updating Metadata within its Data Catalog. The process of metadata update shall be implemented as a workflow in the Data Catalog automated tool and by following the National Data Management Office's Data Catalog Guidelines.	P2

MCM.4.5	**Metadata Quality**	The Entity shall establish and follow a clear process for identifying and addressing quality issues with the Metadata. The Metadata quality management process shall include reporting of identified quality issues and development of remediation actions within defined SLAs. The process shall be implemented as a workflow in the Data Catalog automated tool and by following the National Data Management Office's Data Catalog Guidelines.	P1
MCM.4.6	**Metadata Annotation**	The Entity shall establish a clear process for reviewing on regular basis Metadata annotations (tags, comments) added by users to the Metadata within the Data Catalog. The process shall be implemented as a workflow in the Data Catalog automated tool and by following the National Data Management Office's Data Catalog Guidelines.	P3
MCM.4.7	**Metadata Certification**	The Entity shall establish a clear process for reviewing on regular basis trust certificates assigned by users to the Metadata within the Data Catalog. The process shall be implemented as a workflow in the Data Catalog automated tool and by following the National Data Management Office's Data Catalog Guidelines.	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **MCM.1 Plan**

Domain Name	Data Catalog and Metadata	Domain ID	MCM

Control Name	Data Catalog Automation	Control ID	MCM.5
Control Description	As part of the Data Catalog Automation control, the Entity shall implement Data Catalog automated tool, monitor changes to its Metadata and activity of users within the tool		

Specification #	Specification Name	Control Specification	Priority
MCM.5.1	Data Catalog Automated Tool	The Entity shall implement the Data Catalog automated tool acting as an inventory of the Entity's data assets and supporting automation of Entity's Metadata management. The implementation shall be conducted according to the National Data Management Office's Data Catalog Guidelines.	P2
MCM.5.2	Metadata and Catalog Notifications	The Entity shall monitor changes to its Metadata by setting up automated notifications functionality within the Data Catalog automated tool, to keep the entity's data catalog users aware of any metadata updates	P2
MCM.5.3	Metadata and Catalog Audit Trial	The Entity shall monitor activity of users within the Data Catalog automated tool by setting-up a tracking functionality provided by the tool. Monitoring shall include information about users' logins to the Data Catalog and operations they invoke. The Entity shall store as artifacts the Data Catalog's activity and tracking logs.	P2
MCM.5.4	Tool Versioning	The Entity shall have the Data Catalog automated tool updated to the latest published Vendor release or shall have a plan to update to the latest release reflected in the Data Catalog Development Plan. If the latest release is not applicable to the Entity, the Entity shall have the analysis and a rationale for its release management strategy.	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **MCM.1: Plan**

Domain Name	Data Catalog and Metadata	Domain ID	MCM

Control Name	Performance Management	Control ID	MCM.6
Control Description	As part of the Performance Management control, the Entity shall establish key performance indicators (KPIs) to gather statistics on the adoption of Data Catalog by users and to measure quality of its Metadata		

Specification #	Specification Name	Control Specification	Priority
MCM.6.1	Data Catalog KPIs	The Entity shall establish key performance indicators (KPIs) to gather statistics on the usage and the adoption of the Data Catalog by users. KPIs shall include, at minimum, the following: 1. Number of registered Data Catalog users 2. Number of active Data Catalog users 3. Number of logins to Data Catalog 4. Number of performed metadata queries 5. Number of annotations (tags, comments) added to data assets 6. Number of ratings added to data assets 7. Number of assigned trust certificates to metadata.	P2
MCM.6.2	Metadata Quality KPIs	The Entity shall establish key performance indicators (KPIs) to measure quality of its Metadata. KPIs shall include, at minimum, the following: 1. Completeness (degree to which business glossaries and data dictionaries are completed) 2. Accuracy (degree to which definitions and descriptions align to business context) 3. Consistency (degree to which definitions of Metadata are consistent across Entity).	P2

Version History	
June 2020	Version 1.0

Dependencies	- **MCM.4: Data Lifecycle Management** - **MCM.5: Data Catalog Automation**

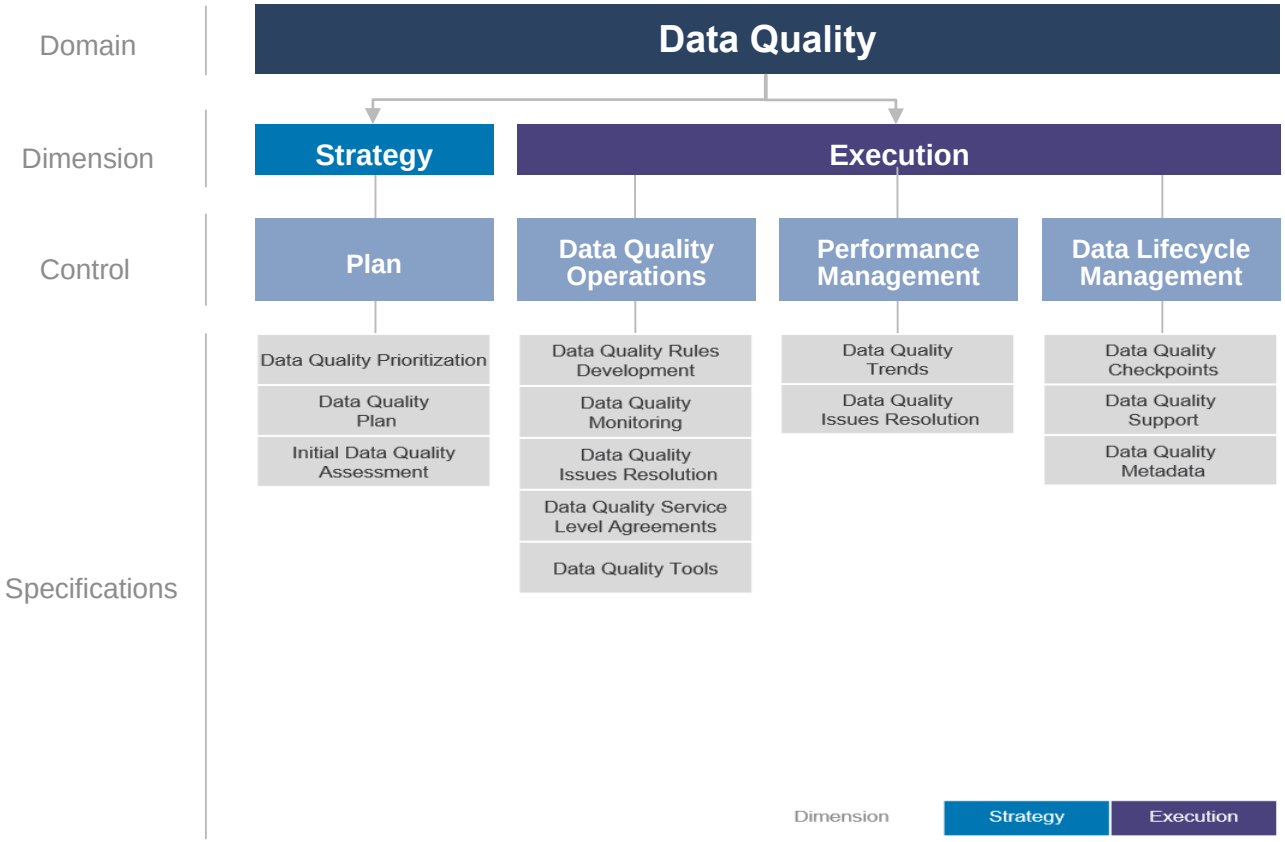
9.2.3. References

Data Catalog and Metadata Domain References	- DAMA DMBOK 2nd Edition (Mosley and Brackett, 2017) - ISO 11179 - ISO 23081 - ISO 10032

9.3. Data Quality Domain

9.3.1. Domain on a Page

Data Quality domain comprises of 4 controls and 13 specifications. This domain Data Quality focuses on the improvement of the quality of the organization data, ensuring that data is fit for purpose based on consumers' requirements.



9.3.2. Controls and Specifications

Domain Name	Data Quality	Domain ID	DQ

Control Name	Plan	Control ID	DQ.1
Control Description	As part of the Plan control, the Entity shall prioritize its data from the perspective of its importance for Data Quality Management, develop a Data Quality Plan and perform an Initial Data Quality Assessment		

Specification #	Specification Name	Control Specification	Priority
DQ.1.1	Data Quality Prioritization	The Entity shall prioritize its data from the perspective of its importance for the Data Quality Management. The result of the prioritization shall be a ranked list of data to be followed when performing the Initial Data Quality Assessment. The 1st priority data shall include, at minimum, the Entity's master data.	P1
DQ.1.2	Data Quality Plan	Based on the Entity's defined Data Management and Personal Data Protection Strategy and Plan, the Entity shall create a Data Quality Plan to implement and manage activities aiming to improve quality of the Entity's data. The plan shall include, at minimum, the following: 1. Roadmap with the activities and key milestones for implementation of the Entity's Data Quality Management. The activities shall, at minimum, incorporate what is needed to achieve the specifications in this domain 2. Assignment of the required resources and budget to manage the implementation of Data Quality management.	P1
DQ.1.3	Initial Data Quality Assessment	The Entity shall perform an Initial Data Quality Assessment of data included in the Entity's Data Quality Management scope. The assessment shall include, at minimum, the following: 1. Collection of business requirements for the Quality of data in the scope	P1

		2. Definition of Data Quality Rules based on collected business requirements 3. Performing of data profiling based on the defined Data Quality Rules 4. Reporting of identified Data Quality issues 5. Development of remediation plans for the identified Data Quality issues. The remediation plan shall include (but not limited to) the following: 5a. Root cause analysis to determine the cause of identified Data Quality issue 5b. Impact analysis to assess negative consequences and a level (local, enterprise-wide) of the issue Definition of the Data Quality targets set for each of the issues, related to each Data Quality dimension, set depending on the issue's context within the entity 5d. Definition of the options for resolving the issue's root cause, including a feasibility analysis 5e. Specification of data cleansing to be performed if Data Quality issue resolution does not correct data 6. Development of a roadmap and key milestones for a resolution of identified Data Quality issues.	

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan**

Domain Name	Data Quality	Domain ID	DQ

Control Name	Data Quality Operations	Control ID	DQ.2
Control Description	As part of the Data Quality Operations control, the Entity shall develop Data Quality Rules, monitor its Data Quality, establish and follow a clear process for resolving the identified Data Quality issues and implement the Data Quality tools		

Specification #	Specification Name	Control Specification	Priority
DQ.2.1	Data Quality Rules Development	The Entity shall develop and document Data Quality Rules for all data included in the Entity's Data Quality Management scope. The rules are used to define the business requirements for Data Quality. The definition of Data Quality Rules shall include, at minimum, the following: 1. Rule owner - the Data Quality Analyst responsible for the rule's definition 2. Business description of the requirement to be validated by the rule 3. Assignment of rules to each of the Data Quality dimensions related to the particular data being measured: 3a. Completeness (the degree to which the necessary data is available for use) 3b. Uniqueness (the degree to which data records are unique, and not duplicates) 3c. Timeliness (the degree to which data is up to date and available when it is needed) 3d. Validity (a degree of records' conformance to format, type and range) 3e. Accuracy (a degree to which data values align to real values) 3f. Consistency (a degree to which data is consistent across different sources) 4. List of data attributes that are validated by the defined rules 5. Metrics that are calculated when the rule is validated (e.g. for the rule validating the completeness of population of the data field, the metrics would be: a number of records	P2

		where data is populated divided by a total number of records) 6. Escalation threshold that triggers a Data Quality alert for the rule (e.g. for the rule validating the completeness of the population of the data field, the escalation threshold could be the alert is triggered when below 90% of records have the field populated).	
DQ.2.2	**Data Quality Monitoring**	The Entity shall monitor and document the Entity's Data Quality on a regular basis based on the defined Data Quality rules. The Data Quality monitoring shall include, at minimum, the following: 1. Execution of existing Data Quality Rules according to defined triggering conditions (time schedule, event) 2. Reporting of the identified Data Quality issues to the Entity's data stewards and owners (at minimum, Business Data Steward and Business Data Executive).	P2
DQ.2.3	**Data Quality Issues Resolution**	The Entity shall establish and follow a clear process for resolving the identified Data Quality issues. The process shall include, at minimum, the following: 1. The development of a remediation plan. The remediation plan shall include, at minimum, the following: 1a. Root cause analysis to determine the cause of the identified Data Quality issue 1b. Impact analysis to assess negative consequences and level (local, enterprise-wide) of the issue 1c. Definition of the options for resolving the issue's root cause, including a feasibility analysis 1d. Specification of data cleansing to be performed if a Data Quality issue resolution does not correct data errors in the source system 2. The decision and rationale on the selected option to resolve the issue 3. The implementation status of the issue's resolution change 4. The review of the implemented change with a verification that the issue is resolved.	P2

DQ.2.4	**Data Quality Service Level Agreements**	The Entity shall establish and implement Data Quality Service Level Agreements specifying the Entity's requirements for resolving the identified Data Quality issues. The Entity's Data Quality Service Level Agreement shall include, at minimum, the following: 1. Timelines and deadlines for the development of the remediation plan for the Data Quality issue 2. Timelines and deadlines for the implementation and the review of Data Quality changes 3. Escalation actions to be taken when the SLA is not met.	P2
DQ.2.5	**Data Quality Tools**	The Entity shall implement tools supporting automation of the Entity's Data Quality Management. The tools shall cover, at minimum, the following capabilities: 1. Data profiling - statistical analysis of data on data attribute, table and cross-domain level 2. Data Quality rules management - a development and an execution of Data Quality rules 3. Data Quality issues management - an automation of workflows for reporting and resolving Data Quality issues.	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **DQ.1: Plan**

Domain Name	Data Quality	Domain ID	DQ

Control Name	Performance Management	Control ID	DQ.3
Control Description	As part of the Performance Management control, the Entity shall establish key performance indicators (KPIs) to measure and report on the Entity's Data Quality trends and on a performance of the Entity's Data Quality issues resolution process		

Specification #	Specification Name	Control Specification	Priority
DQ.3.1	Data Quality Trends	The Entity shall establish key performance indicators (KPIs) to measure and report on the Entity's Data Quality trends against established targets. KPIs shall include, at minimum, the following: 1. Number of Data Quality issues reported based on the implemented Data Quality Rules 2. Number of Data Quality issues reported by the Data Catalog users 3. Number of the Data Quality Rules deployed.	P2
DQ.3.2	Data Quality Issues Resolution	The Entity shall establish key performance indicators (KPIs) to measure and report on a performance of the Entity's Data Quality issues resolution process. KPIs shall include, at minimum, the following: 1. Number of resolved Data Quality issues vs reported Data Quality issues 2. Number of Data Quality issues resolved after the specified deadlines 3. Total time of the development of a Data Quality issue remediation plan 4. Total time of resolving a Data Quality issue (a root cause resolution implementation).	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **DQ.2: Data Quality Operations** - **DQ.4: Data Lifecycle Management**

Domain Name	Data Quality	Domain ID	DQ

Control Name	Data Lifecycle Management	Control ID	DQ.4
Control Description	As part of the Data Lifecycle Management control, the Entity shall publish Data Quality Rules, results of Data Quality monitoring and establish a process for reporting Data Quality issues		

Specification #	Specification Name	Control Specification	Priority
DQ.4.1	Data Quality Checkpoints	The Entity shall have Business and IT Data Stewards conducting the Data Quality reviews within the Software Development Lifecycle (SDLC) process. All Data Quality issues identified during Data Quality reviews shall be remediated before moving to the production. The Data Quality review should include, at minimum, the following: 1. The Data Quality log of identified quality issues 2. The remediation plan for the identified issues.	P2
DQ.4.2	Data Quality Support	The Entity shall establish and follow a clear process enabling data users to report Data Quality issues to the Business Data Stewards. The process shall be implemented as a workflow in the Data Catalog automated tool and following the National Data Management Office's Data Catalog Guidelines.	P3
DQ.4.3	Data Quality Metadata	The Entity shall publish existing Data Quality Rules and results of Data Quality Monitoring as the metadata registered within the Data Catalog automated tool. The population of the metadata shall be executed according to the process defined in Metadata and Data Catalog Management domain.	P3

Version History	
June 2020	**Version 1.0**

Dependencies	- **DQ.1: Plan** - **DG.4: Data Management and Personal Data Protection Organization**

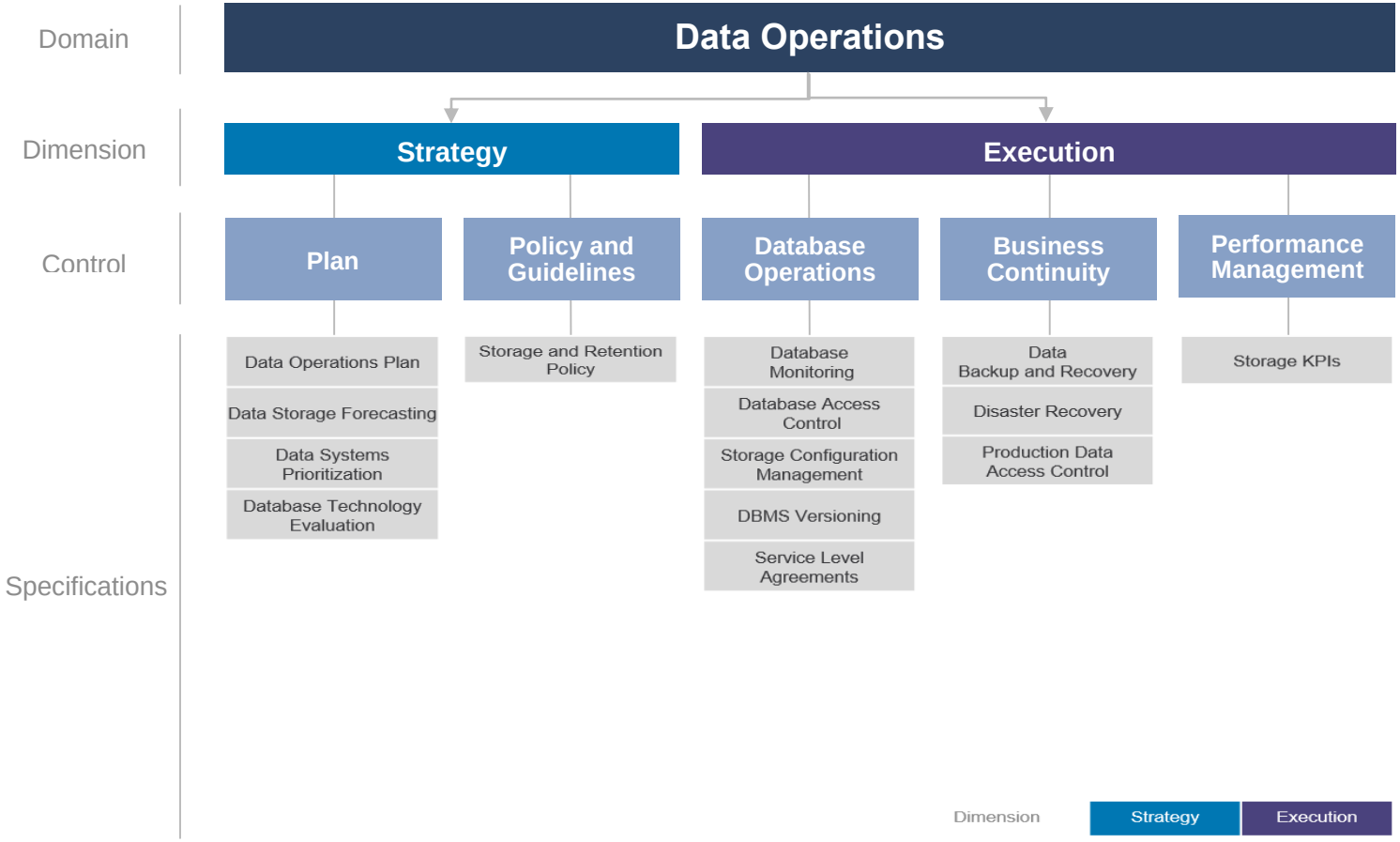
9.3.3. References

Data Quality Domain References	- DAMA DMBOK 2nd Edition (Mosley and Brackett, 2017) - ISO 8000 - Modern Data Strategy ('Fleckenstein and Mike, 2019) - Data Strategy (Marr and Bernard, 2017) - Accenture Data Quality Strategy Playbook (Accenture, 2019)

9.4. Data Operations Domain

9.4.1. Domain on a Page

Data Operations domain comprises of 5 controls and 14 specifications. This domain focuses on the design, implementation, and support for data storage to maximize data value throughout its lifecycle from creation/acquisition to disposal.



9.4.2. Controls and Specifications

Domain Name	Data Operations	Domain ID	DO

Control Name	Plan	Control ID	DO.1
Control Description	As part of the Plan control, the Entity shall create a Data Operation Plan, conduct Data Storage forecasts, prioritize its information systems based on their business criticality and establish and follow a process for evaluation and selection of the Database Management System Software		

Specification #	Specification Name	Control Specification	Priority
DO.1.1	**Data Operations Plan**	Based on the Entity's defined Data Management and Personal Data Protection Strategy and Plan, the Entity shall create a Data Operations Plan to manage and orchestrate Data Operations activities. The plan shall include, at minimum, the following: 1. Roadmap with the activities and key milestones for the implementation of Data Operations initiatives. The activities shall, at minimum, incorporate what is needed to achieve the specifications in this domain 2. Assignment of the required resources and budget to manage the implementation of Data Operations initiatives.	P1
DO.1.2	**Data Storage Forecasting**	The Entity shall conduct periodic forecasts of a storage capacity needed to support future business requirements of the Entity based on: 1. Observation of historical storage trends 2. Assessment of a performance of the Entity's applications 3. The Entity's roadmap for applications' development. Forecasts of a storage capacity shall include, at minimum the following: 1. Prediction of the Entity's future storage capacity needs	P2

		2. Estimation of the budget for future storage acquisitions.	
DO.1.3	**Data Systems Prioritization**	The Entity shall prioritize its information systems based on their business criticality and potential monetary and reputational losses as a consequence of emergency or disaster. The result of the prioritization shall be a list of ranked information systems which shall be used to establish an order of systems recovery in the disaster recovery plan.	P1
DO.1.4	**Database Technology Evaluation**	The Entity shall establish and follow a clear process for evaluation and selection of the Database Management System Software. The process' evaluation factors shall include (but not limited to) the following factors: 1. Total cost of ownership including, at minimum, licensing, support, training, hardware 2. Availability of resources skilled in the technology, both internally and in the market 3. Presence of related software tools in the Entity 4. Volume and velocity limits of the technology 5. Reliability provided by the technology 6. Scalability of the technology 7. Security controls provided by the technology	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan**

Domain Name	Data Operations	Domain ID	DO

Control Name	Policy and Guidelines	Control ID	DO.2
Control Description	As part of the Policy and Guidelines control, the Entity shall create a storage and retention policy for the Data Lifecycle Management of all stored data		

Specification #	Specification Name	Control Specification	Priority
DO.2.1	Storage and Retention Policy	The Entity shall create a storage and retention policy for the Data Lifecycle Management of the Entity's data. The policy shall cover, at minimum, the following areas of the data lifecycle: 1. Storage conditions ensuring a protection of data in the event of disaster 2. Retention periods of data based on its type, classification, business value and legal requirements 3. Disposal and destruction rules based on the data type and classification 4. Required actions in the event of an accidental permanent loss of data.	P1

Version History	
June 2020	Version 1.0

Dependencies	- DG.1: Strategy and Plan

Domain Name	Data Operations	Domain ID	DO

Control Name	Database Operations	Control ID	DO.3
Control Description	As part of the Database Operations control, the Entity shall monitor and report database performance and establish and follow processes for providing the Entity's employees an access to databases and for managing the Entity's Storage Configuration		

Specification #	Specification Name	Control Specification	Priority
DO.3.1	Database Monitoring	The Entity shall monitor and report database performance on regular basis including (but not limited to) the following: 1. Capacity - size of the unused storage 2. Availability - accessibility of databases to users 3. Queries execution performance - query execution times and errors 4. Changes tracking - tracking of database changes for root cause analysis	P2
DO.3.2	Database Access Control	The Entity shall establish and follow a clear process for providing the Entity's employees an access to the databases. The process shall implement a role-based access to the databases which includes an assignment of roles to Entity's employees and granting permissions to the roles. Roles shall be defined by following the data classification domain standards.	P2
DO.3.3	Storage Configuration Management	The Entity shall establish and follow a clear process for managing its Storage Configuration. The process shall include (but not limited to) the following steps: 1. Configuration identification - identification and documentation of the attributes defining the database system configuration 2. Configuration change control - implementation of changes in the defined database configuration	P2

		3. Configuration status accounting - tracking of implemented changes in the configuration 4. Configuration audits - ensuring that the installed database configuration is consistent with the documented configuration	
DO.3.4	**DBMS Versioning**	The Entity shall have its DBMS tools updated to the latest published Vendor release or shall have a plan to update to the latest release reflected in the Data Management and Personal Data Protection Plan. If the latest release is not applicable to the Entity, the Entity shall have the analysis and rationale for its release management strategy.	P3
DO.3.5	**Service Level Agreements**	The Entity shall establish and implement database performance Service Level Agreements specifying the Entity's requirements for the databases performance, data availability and recovery. The Entity's database performance Service Level Agreements shall include (but not limited to) the following: 1. Timeframes for database's availability for users 2. Maximum allowable execution time for selected application transactions 3. Escalation actions to be taken when the SLA is not met	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **DO.1: Plan**

Domain Name	Data Operations	Domain ID	DO

Control Name	Business Continuity	Control ID	DO.4
Control Description	As part of the Business Continuity control, the Entity shall establish and follow a disaster recovery plan and processes for the data backup and recovery and the implementation of database changes to Production Environments		

Specification #	Specification Name	Control Specification	Priority
DO.4.1	Data Backup Recovery	The Entity shall establish and follow a clear process for the data backup and recovery including (but not limited to) the following: 1 - Definition of backup frequency for each information system 2 - Scope of backup for each information system including scope of data and scope of database transaction logs 3 - Location of backup files including a storage medium and a physical location 4 - Periodic validations of backup completions using non-production system copies	P2
DO.4.2	Disaster Recovery	The Entity shall establish and follow a disaster recovery plan including (but not limited to) the following: 1. Prioritized list of information systems defining an order of the information systems recovery 2. Assignment of roles responsible for addressing an incident response 3. Definition of actions to be taken to activate a response to the incident 4. Definition of actions to be taken to reduce the damage and mitigate the consequences of an incident on Entity's critical operations 5. Definition of Recovery Point Objectives (a maximum targeted period within which data might be lost without causing damage to business) for each information system covered in the plan	P2

		6. Definition of Recovery Time Objectives (a maximum targeted duration of time within which database can be down without causing damage to business) for each information system covered in the plan 7. Definition of recovery activities	
DO.4.3	**Production Data Access Control**	The Entity shall establish and follow a clear process for the implementation of database changes to Production Environments. The process shall include (but not limited to) the following: 1. Change request initiating the process 2. Definition of actions to be taken for a controlled implementation of changes to databases 3. Definition of actions to be taken for reversing the changes in case of identified issues	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **DO.2: Policy and Guidelines**

Domain Name	Data Operations	Domain ID	DO

Control Name	Performance Management	Control ID	DO.5
Control Description	As part of the Performance Management control, the Entity shall establish key performance indicators (KPIs) to gather statistics on usage of its data storage		

Specification #	Specification Name	Control Specification	Priority
DO.5.1	Storage KPIs	The Entity shall establish key performance indicators (KPIs) to gather statistics on usage of its data storage. KPIs shall include, at minimum, the following: 1. Percentage of total data storage capacity used 2. Percentage of data storage capacity used by type of database 3. Percentage of data storage capacity used for backups 4. Number of performed data transactions 5. Average time of queries execution.	P2

Version History	
June 2020	Version 1.0

Dependencies	- DO.3: Database Operations

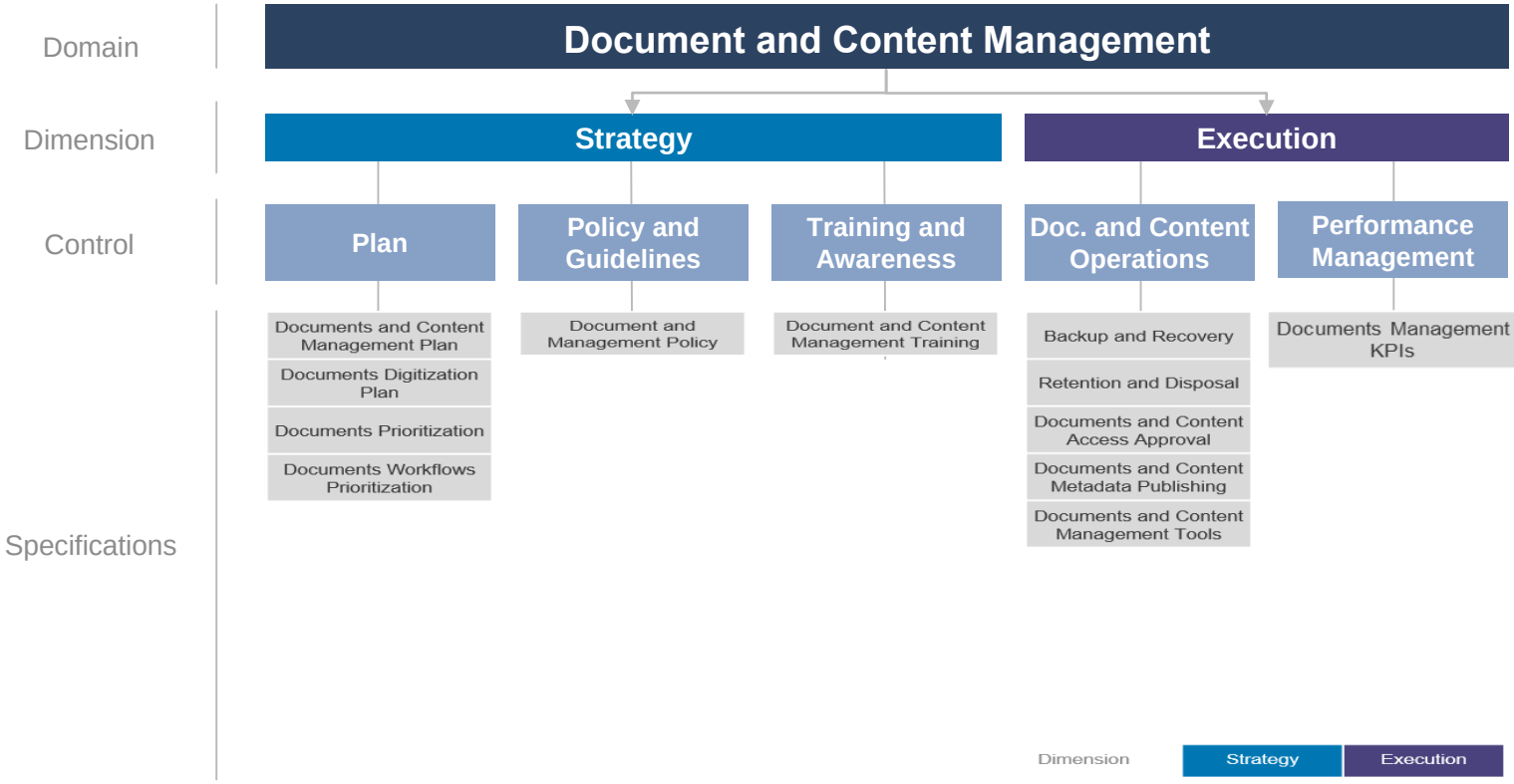
9.4.3. References

Data Operations Domain References	- DAMA DMBOK 2nd Edition (Mosley and Brackett, 2017) - ISO 22301 - Modern Data Strategy ('Fleckenstein and Mike, 2019) - Data Strategy (Marr and Bernard, 2017) - Accenture Data Management Framework (Accenture, 2018)

9.5. Document and Content Management Domain

9.5.1. Domain on a Page

Document and Content Management domain comprises of 5 controls and 12 specifications. This domain involves controlling the capture, storage, access, and use of documents and content stored outside of relational databases.



9.5.2. Controls and Specifications

Domain Name	Document and Content Management	Domain ID	DCM

Control Name	Plan	Control ID	DCM.1
Control Description	As part of the Plan control, the Entity shall create a Document and Content Management Plan and a Documents Digitization Plan as well as prioritize its documents and documents workflows		

Specification #	Specification Name	Control Specification	Priority
DCM.1.1	Document and Content Management Plan	Based on the Entity's defined Data Management and Personal Data Protection Strategy and Plan, the Entity shall create a Document and Content Management Plan to implement and control activities aiming to manage the Entity's documents and content lifecycle. The plan shall include, at minimum, the following: 1. Roadmap with the activities and key milestones for implementation of Documents and Content Management processes. The activities shall, at minimum, incorporate what is needed to achieve the specifications in this domain 2. Assignment of the required resources and budget to manage the implementation of Documents and Content Management processes.	P1

DCM.1.2	**Documents Digitization Plan**	Based on the Entity's defined Data Management and Personal Data Protection Strategy and Plan, the Entity shall create a Documents and Content Digitization Plan to manage the implementation of paperless management initiatives. The plan shall include, at minimum, the following: 1. Roadmap with the activities and key milestones for a migration of the Entity's existing paper-based documents to the electronic format 2. Roadmap with the activities and key milestones for the implementation of initiatives focused on eliminating a creation of paper-based documents in the Entity and replacing them with electronic documents 3. Assignment of the required resources and budget to manage the implementation of paperless management initiatives.	P1
DCM.1.3	**Documents Prioritization**	The Entity shall identify and prioritize its documents to be stored and managed in the Entity's DMS. The result of the prioritization shall be a ranked list of documents to be used as an input in the implementation of the Entity's DMS.	P1
DCM.1.4	**Documents Workflows Prioritization**	The Entity shall identify and prioritize its key processes to be implemented as workflows in DMS to enable automated and paperless management of documents within the Entity. The result of the prioritization shall be a ranked list of the processes to be used as an input in the implementation of the Entity's DMS.	P1

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan**

Domain Name	Document and Content Management	Domain ID	DCM

Control Name	Policy and Guidelines	Control ID	DCM.2
Control Description	As part of the Policy and Guidelines control, the Entity shall create a Document and Content Management policy/policies on managing the data lifecycle for documents and content		

Specification #	Specification Name	Control Specification	Priority
DCM.2.1	Document and Content Management Policy	The Entity shall create a Document and Content Management policy/policies on managing the data lifecycle for documents and content within the Entity. The policy/policies shall cover, at minimum, the following areas of the document and content lifecycle: 1. Documents' naming conventions used 2. Assignment of classification levels to documents 3. Documents and content access approval 4. Documents and content backup and recovery 5. Documents and content retention and disposal	P1

Version History	
June 2020	Version 1.0

Dependencies	- DG.1: Strategy and Plan

Domain Name	Document and Content Management	Domain ID	DCM

Control Name	Training and Awareness	Control ID	DCM.3
Control Description	As part of the Training and Awareness control, the Entity shall conduct document and content management training for the Entity's employees		

Specification #	Specification Name	Control Specification	Priority
DCM.3.1	Document and Content Management Training	The Entity shall conduct the Document and Content Management training for the Entity's employees to increase the awareness on leading practices in the Document and Content Management. The training shall include, at minimum, the following: 1. Introduction of the policies around the Document and Content Management 2. Introductory and advanced tutorials about Document and Content Management systems used and their functionalities.	P2

Version History	
June 2020	Version 1.0

Dependencies	- DCM.1: Plan

Domain Name	Document and Content Management	Domain ID	DCM

Control Name	Document and Content Operations	Control ID	DCM.4
Control Description	As part of the Document and Content Operations control, the Entity shall implement Documents and Content Management Tools, establish and follow processes for retention and disposal of documents and providing employees access to documents and content in the Entity's DMS and CMS		

Specification #	Specification Name	Control Specification	Priority
DCM.4.1	Backup and Recovery	The Entity shall include the Document and Content Management Systems within its overall backup and recovery plan	P3
DCM.4.2	Retention and Disposal	The Entity shall establish and follow a clear process for retention and disposal of the Entity's documents. The process shall implement the Entity's documents retention and disposal policy and shall include (but not limited to) the following: 1. Handover of documents to the Entity's archival facility 2. Physical destruction of documents, including overwriting and a secure deletion	P2
DCM.4.3	Document and Content Access Approval	The Entity shall establish and follow a clear process for providing Entity's employees access to documents and content stored in the Entity's Document and Content Management Systems. The process shall implement a role-based access to documents and content. The CMS and DMS access groups shall be defined by following the Data Classification domain standards	P2
DCM.4.4	Document and Content Metadata Publishing	The Entity shall publish metadata of documents and content stored within the Entity's Document and Content Management Systems in the Entity's Data Catalog automated tool. The population of the metadata shall be executed according to the process defined in Metadata and Data Catalog Management domain.	P3

DCM.4.5	**Documents and Content Management Tools**	The Entity shall implement tools supporting automation of the Entity's Document and Content Management. The tools shall include, at minimum, the following: 1. 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 2. Web Content Management System - an application used to store and manage website Content used by the Entity's portals and internet sites 3. Collaboration tools - applications providing users with platform to collaborate real-time on electronic documents, communicate using chat and track changes in the documents	P3

Version History	
June 2020	**Version 1.0**

Dependencies	- **DCM.1: Plan** - **DCM.2: Policy & Guidelines**

Domain Name	Document and Content Management	Domain ID	DCM

Control Name	Performance Management	Control ID	DCM.5
Control Description	As part of the Performance Management control, the Entity shall define key performance indicators (KPIs) to measure its documents management efficiency		

Specification #	Specification Name	Control Specification	Priority
DCM.5.1	Documents Management KPIs	The Entity shall establish key performance indicators (KPIs) to measure its documents management efficiency. KPIs shall include, at minimum, the following: 1. Volume of the Entity's documents stored and managed within the Entity's Document Management System 2. Number of users of the Entity's Document Management System 3. % of identified paper-based documents migrated to electronic format.	P2

Version History	
June 2020	Version 1.0

Dependencies	- DCM.4: Document and Content Operations

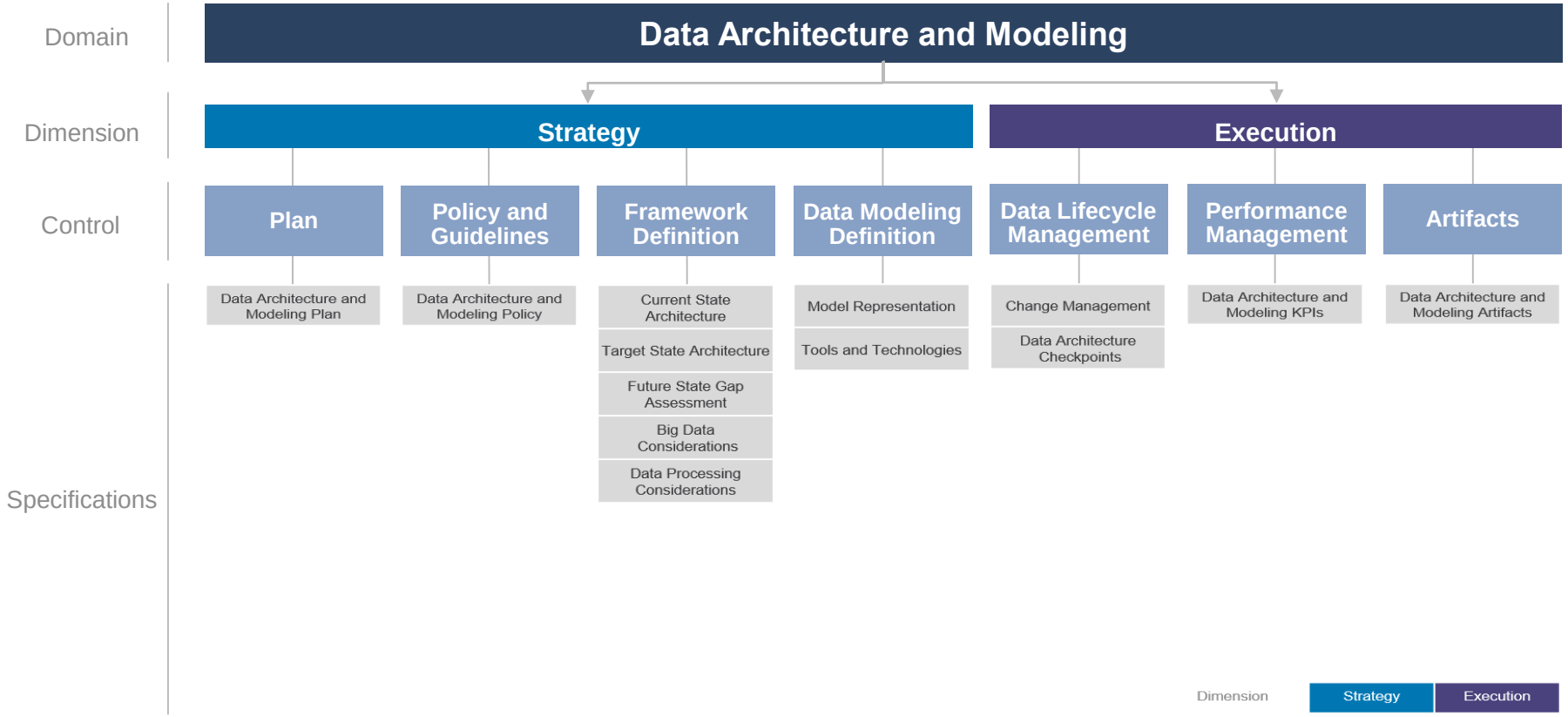
9.5.3. References

Document and Content Management Domain References	- KSA National Center for Archives and Records Regulations - DAMA DMBOK 2nd Edition (Mosley and Brackett, 2017) - Modern Data Strategy ('Fleckenstein and Mike, 2019) - Data Strategy (Marr and Bernard, 2017)

9.6. Data Architecture and Modeling Domain

9.6.1. Domain on a Page

Data Architecture and Modeling domain comprises of 7 controls and 13 specifications. This domain focuses on establishment of formal data structures and data flow channels to enable end to end data processing across and within entities.



9.6.2. Controls and Specifications

Domain Name	Data Architecture and Modeling	Domain ID	DAM

Control Name	Plan	Control ID	DAM.1
Control Description	As part of the Plan control, the Entity shall create a Data Architecture and Modeling Plan to manage the implementation of the target state Data Architecture		

Specification #	Specification Name	Control Specification	Priority
DAM.1.1	Data Architecture and Modeling Plan	Based on the Entity's defined Data Management and Personal Data Protection Strategy and Plan, the Entity shall create a Data Architecture and Modeling Plan to implement and manage activities aiming to improve its Data Architecture Capabilities. The plan shall include, at minimum, the following: 1. Roadmap with the activities and key milestones for the implementation of the target Data Architecture Capabilities. The activities shall, at minimum, incorporate what is needed to achieve the specifications in this domain 2. Assignment of the required resources and budget to manage the implementation of the activities included in the Roadmap.	P1

Version History	
June 2020	Version 1.0

Dependencies	- DG.1: Strategy and Plan

Domain Name	Data Architecture and Modeling	Domain ID	DAM

Control Name	Policy and Guidelines	Control ID	DAM.2
Control Description	As part of Policy and Guidelines control, the Entity shall document and publish a Data Architecture and Modeling Policy		

Specification #	Specification Name	Control Specification	Priority
DAM.2.1	Data Architecture and Modeling Policy	The Entity shall document and publish a Data Architecture and Modeling Policy to guide the development of the target data architecture. The policy shall cover, at minimum, the following: 1. Target Data Architecture shall address strategic requirements defined within the Entity's Data Management and Personal Data Protection Strategy 2. Target Data Architecture shall be developed in conjunction with the development of the Entity's overall Enterprise Architecture 3. Target Data Architecture shall adopt a widely used Enterprise Architecture Framework, e.g. TOGAF, Zachmann 4. The Entity's Data Models shall be monitored regularly and kept up to date.	P1

Version History	
June 2020	Version 1.0

Dependencies	- DG.1: Strategy and Plan

Domain Name	Data Architecture and Modeling	Domain ID	DAM

Control Name	Data Architecture Framework Definition	Control ID	DAM.3
Control Description	As part of the Data Architecture Framework Definition control, the Entity shall define its current and target state Data Architecture and conduct a gap analysis between them, identify and document its requirements for developing a Data Lake environment and define the partitioning strategy for its target state Data Architecture		

Specification #	Specification Name	Control Specification	Priority
DAM.3.1	Current State Architecture	The Entity shall define its 'baseline' current state Data Architecture to support the development of its target state Data Architecture. The current state Data and Technical architecture should cover, at minimum, the following: 1. Data Model - The Entity's current Enterprise Data Model at Conceptual, Logical and Physical level. Each data model level shall cover, at minimum: 1a. Conceptual Model - Key business entities for the Entity with their relationships divided into business subject areas 1b. Logical Model - Conceptual model extended with attributes for business entities and addition of less significant entities and relationships 1c. Physical Model - Physical representation (physical tables names, attributes names, data types, primary and foreign keys etc.) of logical data models within the key System Components 2. Key Processes - Essential current processes involved in ongoing business operations and decision making 3. Key System Components - Essential current applications, data storages, data processing platforms and data analytics solutions involved in key processes	P1

		4. Data Flows and Lineage - Visualized current data movement across the key processes and system components.	
DAM.3.2	**Target State Architecture**	The Entity shall define and develop a future state target data architecture by following the Entity's Data Architecture and Modeling Policy. The target Data Architecture shall cover, at minimum, the following: 1. Data Model - the Entity's target Enterprise Data Model at Conceptual, Logical and Physical level. Each data model level shall include, at minimum: 1a. Conceptual Model - key business entities for the Entity with their relationships divided into business subject areas 1b. Logical Model - conceptual model extended with attributes for business entities and addition of less significant entities and relationships 1c. Physical Model - physical representation (physical tables names, attributes names, data types, primary and foreign keys etc.) of logical data models within the key System Components 2. Key Processes - Essential target processes involved in ongoing business operations and decision making 3. Key System Components - Essential target applications, data storages, data processing platforms and data analytics solutions involved in key processes 4. Data Flows and Lineage - Visualized target data movement across the key processes and system components.	P2
DAM.3.3	**Future State Gap Assessment**	The Entity shall conduct and document a gap analysis between the Entity's current state architecture and the defined target state architecture. The gap analysis shall be used as an input for definition of initiatives required to implement target state data architecture.	P2
DAM.3.4	**Big Data Considerations**	The Entity shall identify and document its requirements for developing a Data Lake environment using a vendor-neutral Big Data	P2

		Reference Architecture Framework (e.g. NIST) and incorporating Big Data architecture components into its overall target Data Architecture design. The Data Lake requirements shall, at minimum, address requirements for: 1. Ingest - Ingesting and converting semi- and unstructured datasets into a structured form 2. Infrastructure - Networking, computing and storage needs handling large, diverse formats of data 3. Platform - Distributed storage solution providing distributed processing capabilities.	
DAM.3.5	**Data Processing Considerations**	The Entity shall employ and document a partitioning strategy for its target state Data Architecture for efficient processing of various data volumes, variety and velocity of data and optimizing data processing and systems performance. The partitioning strategy should cover both real-time and batch processing operations.	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **DAM.1: Plan** - **DAM.2: Policy & Guidelines**

Domain Name	Data Architecture and Modeling	Domain ID	DAM

Control Name	Data Modeling Definition	Control ID	DAM.4
Control Description	As part of the Data Modeling Definition control, the Entity shall select diagramming method for documenting the structure, relationships and notations of business entities and select a toolset of technologies for the implementation of Data Architecture and Modeling initiatives within the Entity		

Specification #	Specification Name	Control Specification	Priority
DAM.4.1	Model Representation	The Entity shall select and follow a diagramming method (e.g. UML) for documenting the structure, relationships and notations of business entities at the conceptual, logical and physical level that can be used throughout the Software Development Lifecycle (SDLC).	P2
DAM.4.2	Tools and Technologies	The Entity shall select and implement a toolset of technologies for the design, development and implementation of data architecture and modeling initiatives within the Entity. The Entity's toolset shall cover, at minimum, the following: 1. Data Architecture Design - Visually representing data and system components along with data flow diagramming 2. Data Modeling - Drawing functionality to create and modify data and system objects, attributes and relationships, and perform reverse engineering of existing data models 3. Data Lineage - Capturing and maintaining of data flows between systems to enable an impact analysis.	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **DAM.1: Plan** - **DAM.2: Policy & Guidelines**

Domain Name	Data Architecture and Modeling	Domain ID	DAM

Control Name	Data Lifecycle Management	Control ID	DAM.5
Control Description	As part of the Data Lifecycle Management control, the Entity shall establish an architecture change management process and follow Data Architecture checkpoints incorporated into its SDLC process		

Specification #	Specification Name	Control Specification	Priority
DAM.5.1	Change Management	The Entity shall establish and follow an architecture change management process to review, approve and implement changes to current and/or target state Data Architectures. The scope of architecture changes shall include, at minimum, the following: 1. Requests for new Data Architecture and Data Modeling initiatives 2. Modifications to Statement of Architecture Work documents for existing initiatives.	P2
DAM.5.2	Data Architecture Checkpoints	The Entity shall have Data Architecture checkpoints incorporated into its Software Development Lifecycle (SDLC) process. The checkpoints shall include, at minimum, the following: 1. Investigation of possibilities for reusage of existing Data Architecture components to address business requirements 2. Validation of conformance of created data models with the Entity's Enterprise Data Model 3. Verification if project implies any changes required to the Entity's overall Enterprise Data Model.	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **DAM.1: Plan** - **DAM.3: Data Architecture Framework Definition** - **DG.4: Data Management & Privacy Organization**

Domain Name	Data Architecture and Modeling	Domain ID	DAM

Control Name	Performance Management	Control ID	DAM.6
Control Description	As part of the Performance Management control, the Entity shall develop key metrics to regularly measure the Entity's Data Architecture and Modeling capabilities		

Specification #	Specification Name	Control Specification	Priority
DAM.6.1	Data Architecture and Modeling KPIs	The Entity shall establish key performance indicators (KPIs) to measure the state of its Data Architecture and Modeling capabilities. KPIs shall include, at minimum, metrics to track progress in transforming current state data architecture towards a target state data architecture.	P2

Version History	
June 2020	Version 1.0

Dependencies	- DAM.3: Data Architecture Framework Definition - DAM.4: Data Modeling Definition - DAM.5: Data Lifecycle Management

Domain Name	Data Architecture and Modeling	Domain ID	DAM

Control Name	Artifacts	Control ID	DAM.7
Control Description	As part of the Artifacts control, the Entity shall store and maintain its Data Architecture documentation materials		

Specification #	Specification Name	Control Specification	Priority
DAM.7.1	Data Architecture and Modeling Register	The Entity shall store in a register its data and technical architecture project, reference documentation materials and data model designs.	P2

Version History	
June 2020	Version 1.0

Dependencies	- DAM.3: Data Architecture Framework Definition - DAM.4: Data Modeling Definition

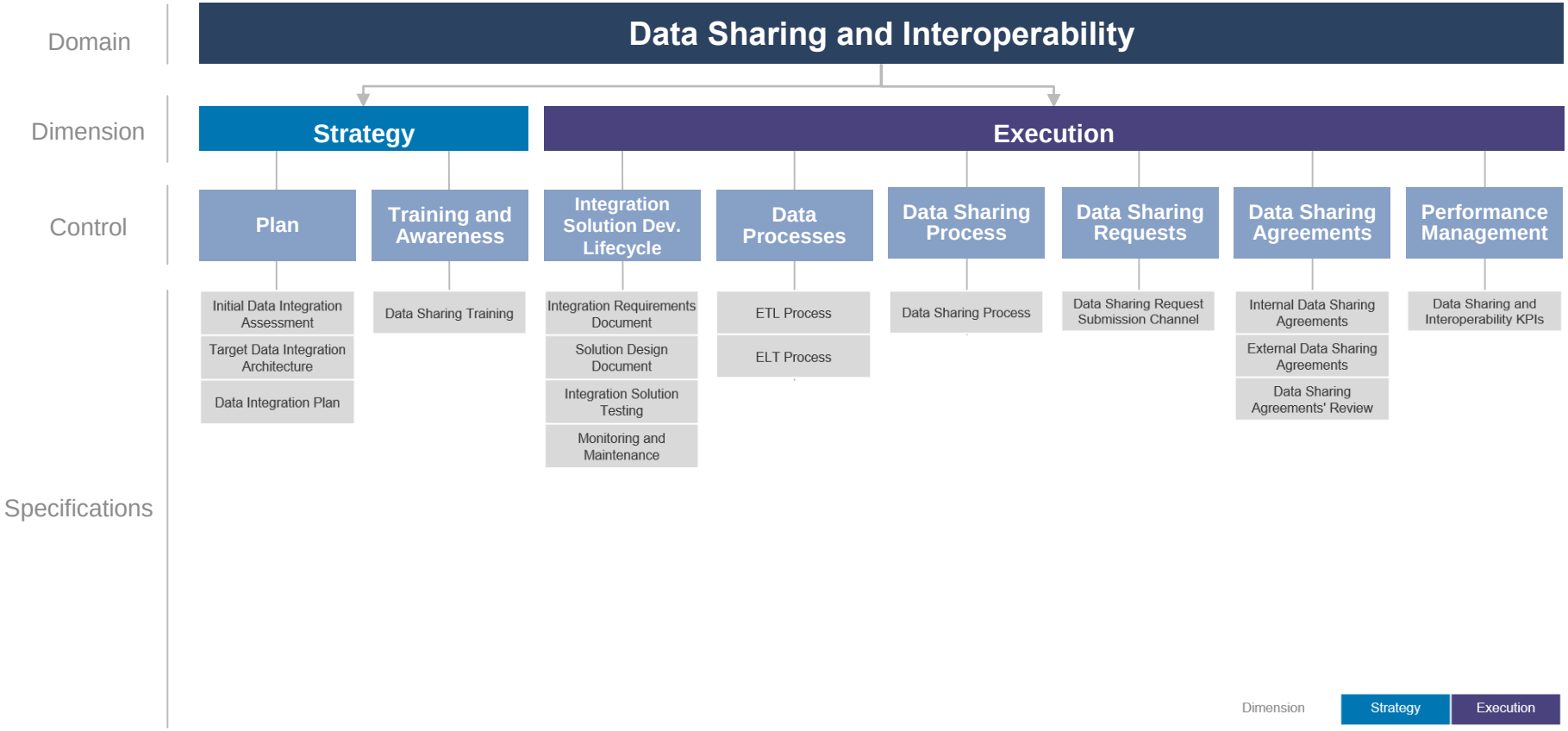
9.6.3. References

Data Architecture and Modeling Domain References	- DAMA DMBOK 2nd Edition (Mosley and Brackett, 2017) - The TOGAF® Standard, Version 9.2 - NIST.SP.1500-5 Big Data Interoperability Framework: Architectures White Paper Survey (NIST.gov, 2015) - Data Architecture Playbook (Accenture, 2017) - Accenture Data Management Framework (Accenture, 2018)

9.7. Data Sharing and Interoperability Domain

9.7.1. Domain on a Page

Data Sharing and Interoperability domain comprises of 8 controls and 16 specifications. This domain involves the collection of data from different sources and consists of integration solutions fostering a harmonious internal and external communication between various IT components. Data Sharing and Interoperability also covers a Data Sharing process that enable an organized and standardized exchange of data between entities



9.7.2. Controls and Specifications

Domain Name	Data Sharing and Interoperability	Domain ID	DSI

Control Name	Plan	Control ID	DSI.1
Control Description	As part of the Plan control, the Entity shall perform an Initial Data Integration Assessment and create a Target Data Integration Architecture and a Data Integration Plan		

Specification #	Specification Name	Control Specification	Priority
DSI.1.1	**Initial Data Integration Assessment**	The Entity shall perform an Initial Data Integration Assessment to identify pain points and inefficiencies in the data movement and the integration across the Entity. The assessment shall include, at minimum, the following: 1. Creating an inventory of all existing IT components (data sources, systems, applications and data stores) 2. Documenting a high-level Data Lineage including the rules according to which data is changed, and the frequency of changes 3. Documenting data models used by the Entity's IT components. The result of the Initial Data Integration Assessment shall be a list of identified data movement and integration pain points.	P1
DSI.1.2	**Target Data Integration Architecture**	The Entity shall create a Target Data Integration Architecture based on the pain points identified in the Initial Data Integration Assessment to manage the data movement efficiently across data stores, systems and applications. At minimum, the Target Data Integration Architecture shall include, the following: 1. Data Integration Requirements - Data Integration Requirements defined by the key business and IT stakeholders (incl. Data Architects)	P1

		2. Data Integration Architecture Diagram - Conceptual architecture diagram that defines the target integration architecture of the Entity's IT components (data sources, systems, applications, data stores) and the integration toward external IT components 3. Architecture Components - List of IT components (data sources, systems, applications, data stores) included in the scope of the Target Data Integration Architecture	
DSI.1.3	**Data Integration Plan**	Based on the Entity's defined Data Management and Personal Data Protection Strategy and Plan, the Entity shall create a Data Integration Plan to identify and orchestrate the implementation of the integration initiatives. The plan shall include, at minimum, the following: 1. Roadmap with the activities and key milestones for the implementation of the Target Data Integration Architecture. The activities shall, at minimum, incorporate what is needed to achieve the specifications in this domain 2. Assignment of the required resources and budget to manage the implementation of the Data Integration initiatives.	P1

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Plan**

Domain Name	Data Sharing and Interoperability	Domain ID	DSI

Control Name	Training and Awareness	Control ID	DSI.2
Control Description	As part of the Training and Awareness control, the Entity conduct training on the Data Sharing to ensure employees involved in the Data Sharing initiatives understand their responsibilities and the consequences of an unauthorized disclosure or mishandling of data		

Specification #	Specification Name	Control Specification	Priority
DSI.2.1	Data Sharing Training	The Entity shall conduct the Data Sharing training for every employee involved in the Data Sharing initiatives to ensure that they understand their obligations, responsibilities and the consequences of an unauthorized disclosure or mishandling of data. The training shall include, at minimum, the following: 1. Introduction on the applicability of the Data Sharing process 2. Leading practices of data handling 3. Consequences of mishandling of data 4. Data Sharing Principles and Controls	P2

Version History	
June 2020	Version 1.0

Dependencies	- DSI.1: Strategy and Plan

Domain Name	Data Sharing and Interoperability	Domain ID	DSI

Control Name	Integration Solution Development Lifecycle	Control ID	DSI.3
Control Description	As part of the Integration Solution Development Lifecycle control, the Entity shall for each data integration initiative produce an Integration Requirements Document, Solution Design Document and test the developed Integration Solution prior to deployment in the Production Environment		

Specification #	Specification Name	Control Specification	Priority
DSI.3.1	Integration Requirements Document	The Entity shall produce an Integration Requirements Document for each Entity's initiative requiring the data integration between the Entity's IT components. The document shall include, at minimum, the following: 1. Clearly defined scope 2. Entity's Business goals and objectives to be achieved 3. Implementation Timeline 4. Resources required 5. Cost estimate 6. Functional Requirements 7. Non-Functional Requirements.	P1
DSI.3.2	Solution Design Document	The Entity shall create a Solution Design Document for each integration initiative based on the Integration Requirements Document provided. The document shall include, at minimum, the following: 1. Integration Solution Overview – Description of the solution supported by the Solution Overview Diagram 2. Target Data Integration Architecture Adherence – Alignment to the Target Data Integration Architecture 3. Data Orchestration – The Data-Flow-Diagram (DFD) portraying the flow of data in a data integration solution from start to finish, including intermediate steps, required to complete the transformation 4. Source-To-Target Mapping - Set of data transformation instructions that determine	P1

		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, at minimum, the following: 4a. The technical format of data at the source and the target 4b. Specification of transformations required for all intermediate staging points between the source and the target.	
DSI.3.3	**Integration Solution Testing**	The Entity shall perform testing of the developed Integration Solution prior to deploying it to the Production Environment to verify that it was implemented as defined in the Solution Design Document. At minimum, testing shall consist of the following stages: 1. Integration Testing – Verifying the correctness of data flows between integrated IT components (systems, applications, data stores) to identify and resolve any Data Quality issues or bugs 2. Functional Testing – Verifying that the system meets both functional and non-functional requirements and satisfies business goals. Each of above stages shall include, at minimum, the following: 1. Defining Test Use Cases 2. Setting up a Test Environment 3. Executing Test Use Cases in a Test Environment and documenting test results.	P2
DSI.3.4	**Monitoring and Maintenance**	The Entity shall actively monitor and maintain the Integration Solution after its release to the Production Environment. The monitoring and maintenance shall include, at minimum, the following: 1. Reporting on any identified bugs or defects 2. Producing the Change Request document to accommodate for any change requirements from the end users.	P3

Version History	
June 2020	**Version 1.0**

Dependencies	- **DSI.1: Plan**

Domain Name	Data Sharing and Interoperability	Domain ID	DSI

Control Name	Data Processes	Control ID	DSI.4
Control Description	As part of the Data Processes control, the Entity shall design, document and follow ETL and ELT processes		

Specification #	Specification Name	Control Specification	Priority
DSI.4.1	ETL Process	The Entity shall design, document and follow ETL (Extract Transform Load) process to integrate data from disparate sources and load it into Data Warehouse Store. The process shall include the following steps: 1. Extract - Data Extraction shall include, at minimum, the following: 1a. Identification of data sources from which the data will be extracted 1b. Extracting data from the data sources 1c. Staging extracted data temporarily in a physical data store on disk or in a memory 2. Transform - Data Transformation shall include, at minimum, the following: 2a. Data Mapping - Planning the actual transformation process 2b. Data Transformation - Removing duplicate data, filling out missing values, filtering, sorting, joining and splitting data 2c. Review - Validating the correctness of the transformation 3. Load - Storing of physically transformed data in the Data Warehouse Store.	P2
DSI.4.2	ELT Process	The Entity shall design, document and follow ELT Process to store the unstructured data in its raw native format in the Data Lake. The process shall include the following steps: 1. Extract - Data Extraction shall include, at minimum, the following: 1a. Identification of data sources from which the data will be extracted 1b. Extracting data from the data sources	P2

		2. Loading - Storing physically data in its raw native format in the Data Lake 3. Transform - Data Transformation shall include, at minimum, the following: 3a. Data Mapping - Planning the actual transformation process 3b. Data Transformation - Removing duplicate data, filling out missing values, filtering, sorting, joining and splitting data 3c. Review - Validating the correctness of the transformation.	

Version History	
June 2020	**Version 1.0**

Dependencies	- **DSI.1: Plan** - **DG.4: Data Management & Privacy Organization** - **DO: Data Operations**

Domain Name	Data Sharing and Interoperability	Domain ID	DSI

Control Name	Data Sharing Process	Control ID	DSI.5
Control Description	As part of the Data Sharing Process control, the Entity shall adopt the Data Sharing Process as defined in the Data Sharing Regulation published by the National Data Management Office		

Specification #	Specification Name	Control Specification	Priority
DSI.5.1	Data Sharing Process	The Entity shall adopt and follow the Data Sharing Process as defined in the Data Sharing Regulation published by the National Data Management Office when sharing data externally with Public Entities, Private Organizations and Individuals. The Data Sharing Process shall include the following steps: 1. Data Sharing Request Reception 2. Roles assignment 3. Data Classification level check 4. Data Sharing Principles assessment 5. Data Sharing decision and feedback 6. Business Data Executive approval 7. Design and implementation of Data Sharing controls 8. Data Sharing agreement signing 9. Sharing data with the Requestor.	P1

Version History	
June 2020	Version 1.0

Dependencies	- **DSI.1: Plan** - **DG.4: Data Management and Personal Data Protection Organization**

Domain Name	Data Sharing and Interoperability	Domain ID	DSI

Control Name	Data Sharing Requests	Control ID	DSI.6
Control Description	As part of the Data Sharing Requests control, the Entity shall establish a request submission channel on its official Government website to manage the reception of Data Sharing requests		

Specification #	Specification Name	Control Specification	Priority
DSI.6.1	Data Sharing Request Submission Channel	The Entity shall establish on its official Government website a channel to manage the submission and the reception of Data Sharing requests. Each such request shall be routed to the Data Office.	P1

Version History	
June 2020	Version 1.0

Dependencies	- DSI.5: Data Sharing Process

Domain Name	Data Sharing and Interoperability	Domain ID	DSI

Control Name	Data Sharing Agreements	Control ID	DSI.7
Control Description	As part of the Data Sharing Agreements control, the Entity shall design, implement and review Data Sharing Agreements		

Specification #	Specification Name	Control Specification	Priority
DSI.7.1	Internal Data Sharing Agreements	The Entity shall define and follow an Internal Data Sharing agreement template that shall be used when data is shared between information systems within the Entity.	P2
DSI.7.2	External Data Sharing Agreements	The Entity shall design and implement the required Data Sharing controls as defined in the Data Sharing Regulation. The controls shall be agreed with the requesting Entity, and they shall be documented in the Data Sharing Agreement. The Data Sharing Agreement shall include, at minimum, the following: 1. Purpose of the Data Sharing 2. Information about requesting and sharing Entity 3. Lawful basis for sharing 4. Sharing details (date, duration) 5. Liability provisions The Data Sharing agreement shall be signed by the Business Data Executive and the Requestor prior to sharing data.	P1
DSI.7.3	Data Sharing Agreements' Review	The Entity shall review all ongoing Data Sharing agreements on a regular basis to accommodate for any changes. The audit shall be executed, and its outcome documented by the Data Steward based on contractual provisions and procedures detailed out in the Data Sharing agreement.	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **DSI.5: Data Sharing Process** - **DG.4: Data Management and Personal Data Protection Organization**

Domain Name	Data Sharing and Interoperability	Domain ID	DSI

Control Name	Performance Management	Control ID	DSI.8
Control Description	As part of Performance Management control, the Entity shall define and implement KPIs to measure the progress and benefits from implementing Data Integration solutions and the effectiveness of Data Sharing activities		

Specification #	Specification Name	Control Specification	Priority
DSI.8.1	Data Sharing and Interoperability KPIs	The Entity shall establish key performance indicators (KPIs) to measure the progress and benefits from implementing Data Integration solutions, and the effectiveness of Data Sharing activities. KPIs shall include, at minimum, the following: 1. Data transfer rate between systems / applications 2. Latency between data sources and data targets 3. The number of Data Sharing requests received 4. The number of Data Sharing requests accepted/denied 5. The number of Data Sharing requests sent 6. The number of ongoing Data Sharing agreements 7. Average duration of Data Sharing requests evaluation process expressed in days.	P2

Version History	
June 2020	Version 1.0

Dependencies	- DSI.3: Integration Solution Development Lifecycle - DSI.5: Data Sharing Process

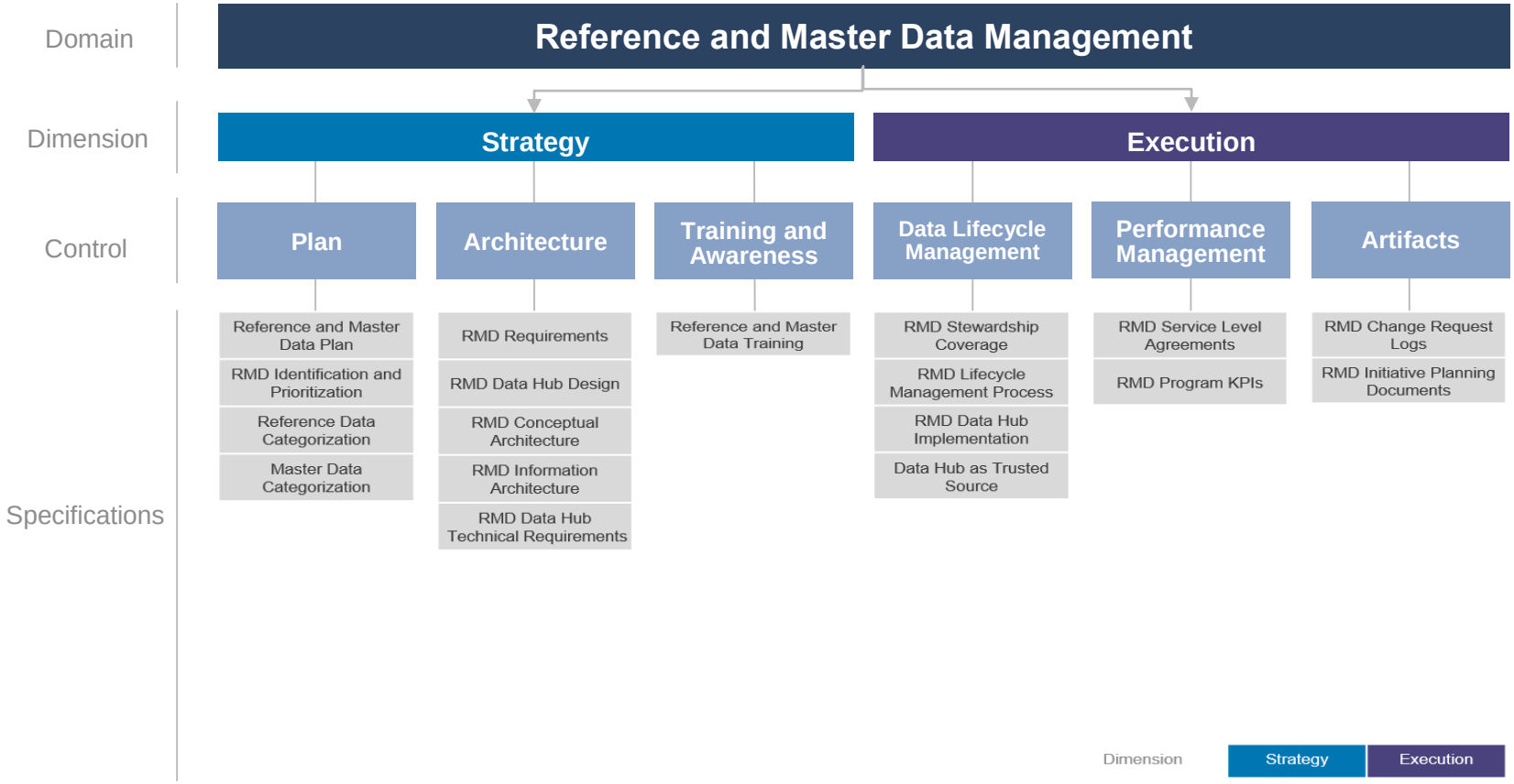
9.7.3. References

Data Sharing and Interoperability Domain References	- DAMA DMBOK 2nd Edition (Mosley and Brackett, 2017) - National Data Management Office's Data Sharing Regulation - National Data Management Office's Data Classification Regulation - NIST.SP.1500-1 Big Data Interoperability Framework Definitions (NIST.gove, 2015) - Modern Data Strategy ('Fleckenstein and Mike, 2019) - Accenture Data Management Framework (Accenture, 2018)

9.8. Reference and Master Data Management Domain

9.8.1. Domain on a Page

Reference and Master Data Management domain comprises of 6 controls and 18 specifications. This domain allows to link all critical data to a single master file, providing a common point of reference for all critical data.



9.8.2. Controls and Specifications

Domain Name	Reference and Master Data Management	Domain ID	RMD

Control Name	Plan	Control ID	RMD.1
Control Description	As part of the Plan control, the Entity shall develop a Reference and Master Data Plan to manage the implementation of the target RMD Information Architecture, identify, document and prioritize Reference and Master data objects owned by the Entity and categorize them as either internal or external datasets		

Specification #	Specification Name	Control Specification	Priority
RMD.1.1	Reference and Master Data Plan	Based on the Entity's defined Data Management and Personal Data Protection Strategy and Plan, the Entity shall create a Reference and Master Data Plan to implement and manage activities aiming to improve its Reference and Master Data Management Capabilities. The plan shall include, at minimum, the following: 1. Roadmap with the activities and key milestones for the implementation of the Entity's Reference and Master Data Management. The activities shall, at minimum, incorporate what is needed to achieve the specifications in this domain 2. Assignment of the required resources and budget to manage the implementation of the activities included in the Roadmap.	P1
RMD.1.2	Reference and Master Data Identification and Prioritization	The Entity shall identify its reference and master data. The identification shall cover, at minimum, the following: 1. Identification of Master Data objects (e.g. customer, product, citizen) used across the Entity 2. Identification of Reference Data Objects required by instances of identified Master Data Objects 3. Identification of data sources and applications where Reference and Master	P1

		Data Objects are created, read, updated and deleted. The Entity shall logically group and prioritize its identified Reference and Master Data Objects for determining a phased approach to implementation of target RMD Information Architecture.	
RMD.1.3	**Reference Data Categorization**	The Entity shall categorize its identified Reference Data Objects as either internal or external datasets: - Internal - Any reference data the Entity owns, manages and is Single Source of Truth across government - External - Any reference data owned and managed by other Entities across government or considered standard industry data coming from external organizations such as ISO. An identification of internal and external reference data used by the Entity is as an input for standardization activities of Reference Data at the national Government level.	P1
RMD.1.4	**Master Data Categorization**	The Entity shall categorize its identified Master Data objects as either internal or external: - Internal - Any Master Data Objects the Entity owns, manages and is Single Source of Truth across government - External - Any Master Data Objects owned and managed by other Entities across government. An identification of internal and external Master Data Objects used by the Entity is as an input for standardization activities of Master Data at the national Government level.	P1

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan**

Domain Name	Reference and Master Data Management	Domain ID	RMD

Control Name	Architecture	Control ID	RMD.2
Control Description	As part of the Architecture control, the Entity shall develop and document its requirements for effectively managing its Reference and Master Data, evaluate and select a Reference and Master Data Hub architecture design, develop a conceptual and an information architectures for its target Reference and Master Data environment, and document the technical requirements for its Reference and Master Data Hub platform		

Specification #	Specification Name	Control Specification	Priority
RMD.2.1	RMD Requirements	Based on the Data Management and Personal Data Protection Strategy, the Entity shall establish and document its requirements for effectively managing the Entity's Reference and Master Data across the data lifecycle. The requirements for Reference and Master Data shall cover, at minimum, the following: 1. Processes and related roles for managing the Entity's Reference and Master Data Objects across the data lifecycle from creation to archiving 2. Rules for accurate matching and merging Master Data Records from different data sources to create Golden Record 3. Requirements for provisioning of Master Data Golden Records to consuming applications 4. Requirements for provisioning of Reference Data Objects to consuming applications 5. Data quality requirements for Reference and Master Data Objects to be leveraged an input for Initial Data Quality Assessment detailed in Data Quality domain.	P1
RMD.2.2	RMD Data Hub Design	The Entity shall evaluate and select Reference Master Data Hub architecture design to effectively manage its Reference and Master	P1

		Data Objects. The Entity shall determine, based on its RMD Requirements, which of the following Data Hub architecture implementation patterns is most suitable for managing its Master Data Objects: 1. Registry Hub - Master Data Records remains in its respective source systems. The Hub stores an index of Master Data with key identifiers only. Creating and modifying master data is maintained in the Master Data sources, the Hub provides links to Master Data Records in data sources 2. Repository Hub - Master Data Records are copied from source systems, matched and consolidated into the Data Hub. Master Data is pushed out (one-way synchronization) to the Data Hub from existing sources. Creating and modifying of Master Data Records is maintained in the Master Data sources 3. Coexistence Hub - Two-way synchronization is added to the Repository Hub design to ensure both source and Hub maintain exactly the same replicas of Master Data Records over time. Creating and modifying of Master Data Records is maintained in the respective data sources 4. Centralized Hub - Master Data Records are migrated to the Data Hub. The Hub becomes the exclusive, single provider of Master Data Records with creating and modifying performed exclusively in the Hub. All consumer applications use the Hub exclusively for their Master Data. Regarding Reference Master Data Objects, the Hub Design shall support Centralized management of Reference Data - the Hub acting as a single provider of Reference Data with creating and modifying performed exclusively in the Hub. All consumer applications use the Hub as a provider of Reference Data.	
RMD.2.3	**RMD Conceptual Architecture**	The Entity shall develop and document a conceptual architecture for its target Reference and Master Data environment per the Entity's selected Data Hub architecture design. The conceptual architecture shall indicate foundational building block components and	P1

		high-level capabilities associated with the components. The conceptual 'RMD' architecture shall consist, at minimum, of the following: 1. Architecture Description - Description of the overall architecture concept defined 2. Components Definitions and Descriptions - Building blocks (the Data Hub, data sources, consuming applications etc.) of RMD conceptual architecture with description of their purpose 3. Conceptual Architecture Diagram- High level view of how components work together to address the Entity's RMD requirements.	
RMD.2.4	**RMD Information Architecture**	The Entity shall develop and document an information architecture for its target Reference and Master Data environment based on defined conceptual architecture. The information architecture shall represent, at minimum, the following components: 1. Reference and Master Data Objects - inventory of identified Reference and Master Data Objects including metadata definitions 2. Conceptual and Logical Master Data Model - conceptual and logical data model for identified Master Data Objects and their relationships 3. Reference and Master Data Sources - Inventory of identified reference and master data sources 4. Rules for matching and merging Master Data Records from different data sources to create Golden Record within the Data Hub 5. Reference and Master Data Flows - One way or bi-directional data movements of: 5a. Master Data Records between data sources and the Data Hub 5b. Master Data Golden Records between Data Hub and consuming applications 5c. Reference Data between Data Hub and consuming applications.	P2
RMD.2.5	**RMD Data Hub Technical Requirements**	The Entity shall define and document the technical requirements for its Reference and Master Data Hub platform based on the defined target RDM Information Architecture. The	P2

		requirements shall cover, at minimum, the following areas: 1. Management of Workflows - Creating and modifying of Reference and Master Data Records and assignment of the MDM stewardship 2. Versioning Control - Tracking of changes to Reference and Master Data Records over time 3. Functional Capabilities - Functional capabilities required from the Hub (e.g. Import, export and mappings of data, automation of operational tasks around collection, cleansing etc.) 4. Technical Capabilities - Technical capabilities required from the Hub (e.g. API Integration with upstream and downstream applications and systems) 5. Security - Support for secure data exchange between the Hub and connected applications/data sources.	

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan**

Domain Name	Reference and Master Data Management	Domain ID	RMD

Control Name	Training and Awareness	Control ID	RMD.3
Control Description	As part of the Training and Awareness control, the Entity shall conduct Reference and Master Data training for employees responsible for managing reference and master data		

Specification #	Specification Name	Control Specification	Priority
RMD.3.1	Reference and Master Data Training	The Entity shall conduct the Reference and Master Data training for employees responsible for managing Reference and Master Data. The training shall include, at minimum, the following topics: 1. Identification - Identifying correct sources of Master and Reference Data 2. Matching - Linking records between systems containing Master Data 3. Consolidation - Removing duplication and overlap between Master Data Sources 4. Conflict Resolution - Resolving conflicts in Reference and Master Data 5. Managing Changes - Leveraging supporting technologies in managing and automating Reference and Master Data changes.	P2

Version History	
June 2020	Version 1.0

Dependencies	- RMD.1: Plan

Domain Name	Reference and Master Data Management	Domain ID	RMD

Control Name	Data Lifecycle Management	Control ID	RMD.4
Control Description	As part of the Data Lifecycle Management control, the Entity shall assign Data Stewards to all identified RMD Data Objects, establish and follow Data Lifecycle Management process for RMD Data Objects, implement the Reference and Master Data Hub as the Entity's Trusted Source as well as document and maintain its Reference and Master Data Integration Mappings		

Specification #	Specification Name	Control Specification	Priority
RMD.4.1	RMD Stewardship Coverage	The Entity shall assign Business and IT Data Stewards to all identified Reference and Master Data Objects.	P1
RMD.4.2	RMD Data Lifecycle Management Process	The Entity shall establish and follow a clear process for managing Reference and Master Data Objects across Data Lifecycle from creation to archiving. The process shall cover roles and actions involved in, at minimum, the following steps of Data Lifecycle: 1. Creation of new Reference and Master Data Objects and their instances 2. Modification of existing Reference and Master Data Objects and their instances 3. Archiving of Reference and Master Data Objects and their instances	P2
RMD.4.3	RMD Data Hub Implementation	The Entity shall implement the Reference and Master Data Hub for managing its Reference and Master Data Objects and provide Trusted Source of reference and master data across entity. As a part of implementation of the Data Hub, the Entity shall, at minimum: 1. Instantiate the physical Data Hub technical architecture components necessary to address the Entity's target RMD information architecture requirements	P2

		2. Establish the Master Data Model as defined by RMD Information Architecture within the Data Hub 3. Load the Reference and Master Data Objects into the Data Hub 4. Activate necessary replication between Master Data Source systems and the Data Hub 5. Activate synchronization between the Data Hub and consuming applications.	
RMD.4.4	**Data Hub as Trusted Source**	The Entity shall establish the Data Hub as the Entity's Trusted Source for any new information system and application implemented requiring the use of the Entity's Reference and/or Master Data Objects.	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **RMD.1: Plan** - **DG.4: Data Management and Personal Data Protection Organization**

Domain Name	Reference and Master Data Management	Domain ID	RMD

Control Name	Performance Management	Control ID	RMD.5
Control Description	As part of the Performance Management control, the Entity shall establish Service Level Agreements for its Reference and Master Data requests and establish Key Performance Indicators (KPIs) to measure the effectiveness of development of its Reference and Master Data capabilities		

Specification #	Specification Name	Control Specification	Priority
RMD.5.1	RMD Service Level Agreements	The Entity shall establish Service Level Agreements for its RMD Data Lifecycle Management Process to effectively balance time vs. cost for changes to its Reference and Master Data.	P2
RMD.5.2	RMD Program KPIs	The Entity shall establish key performance indicators (KPIs) to measure the effectiveness of development of its Reference and Master Data capabilities. KPIs shall include, at minimum, the following: 1. Number of incorrect data values in the Master Data Records 2. Mean Time to Repair (MTTR) Reference and Master Data quality issues 3. Change request volumes for Reference and Master Data Objects.	P2

Version History	
June 2020	Version 1.0

Dependencies	- RMD.4: Data Lifecycle Management

Domain Name	Reference and Master Data Management	Domain ID	RMD

Control Name	Artifacts	Control ID	RMD.6
Control Description	As part of the Artifacts control, the Entity document in a register a historical record of its change request logs and Reference and Master Data initiative plans		

Specification #	Specification Name	Control Specification	Priority
RMD.6.1	RMD Change Request Logs	The Entity shall document in a register its reference and master data change request logs and the decisions made based on those requests.	P2
RMD.6.2	RMD Initiative Planning Documents	The Entity shall document in a register Statement of Architecture Work documents for its Reference and Master Data initiatives.	P2

Version History	
June 2020	Version 1.0

Dependencies	- RMD.2: Architecture

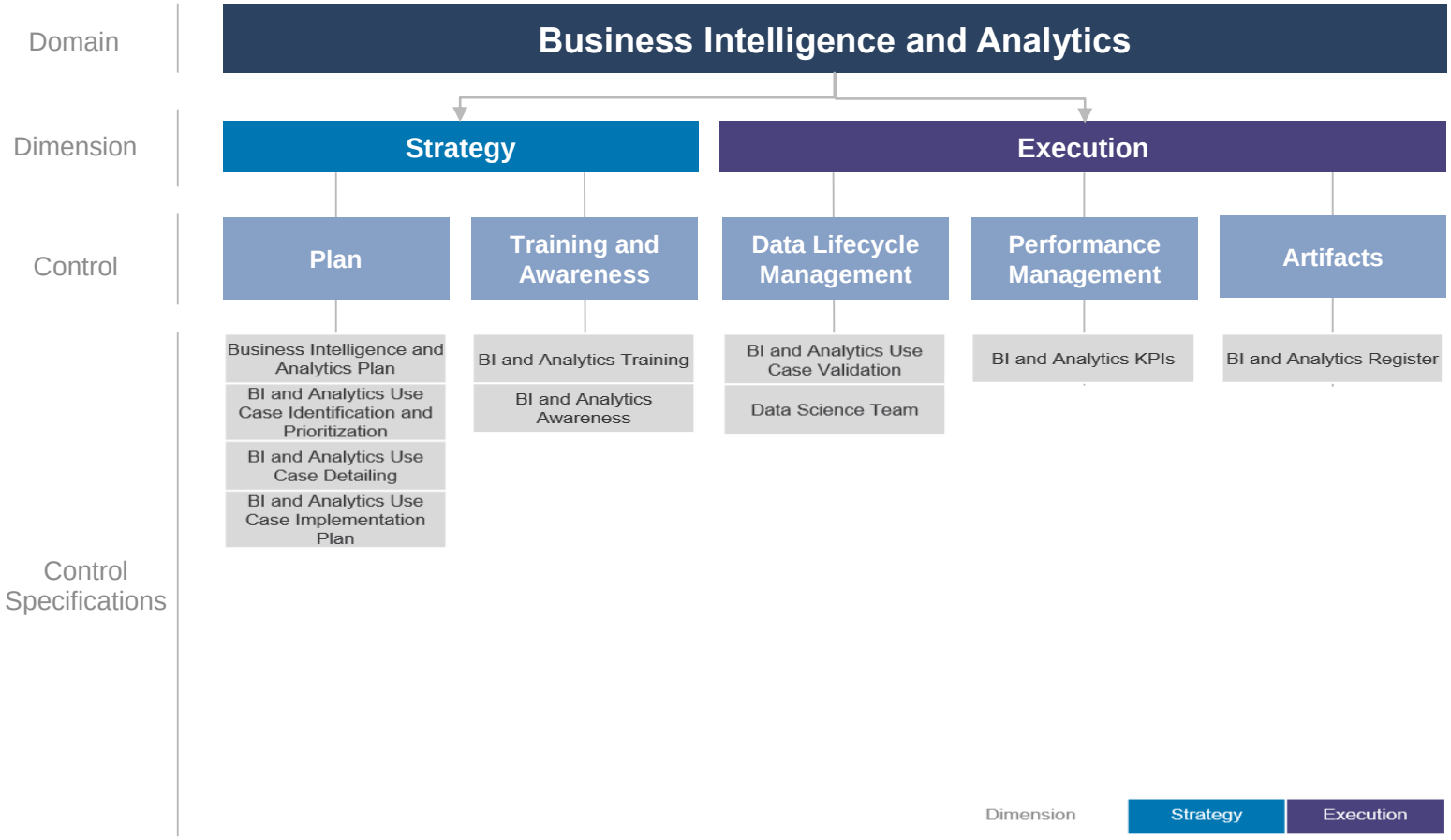
9.8.3. References

Reference and Master Data Domain References	- DAMA DMBOK 2nd Edition (Mosley and Brackett, 2017) - Mastering Master Data Management (Gartner, 2016) - Developing the Best Metrics for Successful Master Data Management (Gartner, 2019) - Implementing the Data Hub: Architecture and Technology Choices (Gartner, 2018) - Master Data Management & Data Governance (Berson, Alex; Dubov, Larry, 2011)

9.9. Business Intelligence and Analytics Domain

9.9.1. Domain on a Page

Business Intelligence and Analytics domain comprises of 5 controls and 10 specifications. This domain focuses on analyzing organization's data records to extract insight and to draw conclusions about the information uncovered



9.9.2. Controls and Specifications

Domain Name	Business Intelligence and Analytics	Domain ID	BIA

Control Name	Plan	Control ID	BIA.1
Control Description	As part of the Plan control, the Entity shall create a Business Intelligence and Analytics Plan, prioritize the list of Analytics and AI use cases and develop an implementation plan for the Analytics and AI Use Cases defined in the use case portfolio		

Specification #	Specification Name	Control Specification	Priority
BIA.1.1	Business Intelligence and Analytics Plan	Based on the Entity's defined Data Management and Personal Data Protection Strategy and Plan, the Entity shall create a Business Intelligence and Analytics Plan to manage and orchestrate Business Intelligence and Analytics activities. The plan shall include, at minimum, the following: 1. Roadmap with the activities and key milestones for the implementation of BI and Analytics use cases. The activities shall, at minimum, incorporate what is needed to achieve the specifications in this domain 2. Assignment of the required resources and budget to manage the implementation BI and Analytics use cases	P1
BIA.1.2	Bi and Analytics Use Case Identification and Prioritization	The Entity shall identify and prioritize the list of BI and Analytics use cases based on the Entity's strategy and key challenges faced within the sector: 1. Identify: Ideation workshops shall be conducted with a long list of identified use cases documented, with each use case defined with its name, description, and entities to be involved in this use case 2. Prioritization: The long list of use cases shall be shortlisted based on a predefined	P1

		prioritization framework with criteria such as impact and complexity	
BIA.1.3	**BI and Analytics Use Case Detailing**	The Entity shall detail the shortlisted BI and Analytics Use Cases that represent the Entity's business data-driven needs. Each shortlisted Analytics Use Case shall, at minimum, have the following documented: 1. Objective aimed to be achieved from the use case 2. Type of Analytics leveraged (among the five maturity levels of discovery, descriptive, diagnostic, predictive, prescriptive) 3. The expected benefits and business value aimed to be derived (ROI) through development of a business case 4. Stakeholders involved in the implementation of the use case, the owner that would lead the use case, and the target consumers that would benefit from the insights generated by the use case 5. List of business requirements to implement the use case 6. Data sources that would feed the use case with the required data fields 7. The technologies required to implement the use cases The long list of use cases, their prioritization, and detailing shall be inserted in a use case portfolio document.	P1
BIA.1.4	**BI and Analytics Use Case Implementation Plan**	The Entity shall develop and document an implementation plan for each the shortlisted and approved BI and Analytics Use Cases defined in the use case portfolio and comprise of the next steps to pilot the use case, followed by production and then monitoring results. The implementation plan shall address, at minimum: 1. Detail Functional and Non-Functional Requirements - Use case objectives translated into analytics requirements 2. High Level Design - Conceptual design of the analytics solution, e.g. wireframes 3. Staging and Production Environment Preparations - Analytics solution hosting environments during and after development	P1

		4. Development - Functional and non-functional requirements to be developed to meet the high-level design 5. Testing - Scope and types of testing to be conducted 6. Deployment and Schedule - Timeline for establishing a pilot and / or delivery of the complete use case 7. Required Resources - Key personnel within the Entity who have the needed skills, expertise and knowledge to successfully implement the Analytics Use Case 8. Acceptance Criteria - Key criteria for measuring the successful implementation of the analytics use case.	

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan**

Domain Name	Business Intelligence and Analytics	Domain ID	BIA

Control Name	Training and Awareness	Control ID	BIA.2
Control Description	As part of the Training and Awareness control, the Entity shall conduct Business Intelligence and Analytics training and create Business Intelligence and Analytics awareness campaigns		

Specification #	Specification Name	Control Specification	Priority
BIA.2.1	Business Intelligence and Analytics Training	The Entity shall conduct the BI and Analytics training for all employees involved in BI and Analytics initiatives to upskill analytics capabilities within the Entity. The training shall include, at minimum, the following: 1. Methods for gathering and organizing data required for the analysis 2. Model development, applying analytics methods and using analytics tools 3. Data models and data flows development 4. Types of graphical representation of data and information 5. Analytical models' evaluation techniques.	P2
BIA.2.2	Business Intelligence and Analytics Awareness	The Entity shall develop and implement Business Intelligence and Analytics awareness campaigns to promote the awareness, education and adoption of its Business Intelligence and Analytics capabilities. Awareness campaigns shall leverage one or more of the Entity's existing communications channels to drive awareness of the Entity's: 1. Current Analytics Assets Available from the Entity - Previously implemented use cases, analytics models, APIs, BI reports and dashboards for potential data sharing and reuse 2. BI and Analytics Success Stories - Quantifiable and qualitative benefits and outcomes from recent use case implementations	P2

		3. New Analytics and AI Tools and Workflows - New Analytics and AI tools and workflows introduced within the Entity, particularly with emerging technologies	

Version History	
June 2020	**Version 1.0**

Dependencies	- **BIA.1: Strategy and Plan**

Domain Name	Business Intelligence and Analytics	Domain ID	BIA

Control Name	Data Lifecycle Management	Control ID	BIA.3
Control Description	As part of the Data Lifecycle Management control, the Entity shall define and conduct a validation process to validate use cases outcomes and shall leverage a data science team to implement them		

Specification #	Specification Name	Control Specification	Priority
BIA.3.1	Business Intelligence and Analytics Use Case Validation	The Entity shall define and conduct a validation process to validate use case outcomes, initial intended purpose and alignment with the Entity's overall Analytics Plan. The validation of use cases, at minimum, shall address: 1. Analytics Use Case functional and non-functional requirements 2. Analytics Use Case Personal Data Protection considerations, as prescribed in the Privacy Domain 3. Analytics Use Case return on investment as per the target set	P2
BIA.3.2	Data Science Team	The Entity shall leverage a Data Analytics Team that would drive the implementation of the Business Intelligence and Analytics specifications. The Data Analytics Team typically include roles such as Data Scientists, Data Engineers, and Visualization Engineers.	P2

Version History	
June 2020	Version 1.0

Dependencies	- BIA.1: Strategy and Plan

Domain Name	Business Intelligence and Analytics	Domain ID	BIA

Control Name	Performance Management	Control ID	BIA.4
Control Description	As part of the Performance Management control, the Entity shall establish key performance indicators (KPIs) to measure performance and effectiveness of its Analytics and AI portfolio		

Specification #	Specification Name	Control Specification	Priority
BIA.4.1	Business Intelligence and Analytics KPIs	The Entity shall establish key performance indicators (KPIs) to measure the performance and effectiveness of its Analytics and AI portfolio. KPIs shall include, at minimum, the following: 1. Number of use cases defined 2. Number of use cases piloted 3. Number of use cases implemented and scaled 4. Total ROI value generated from the implemented use cases 5. Training and awareness sessions delivered.	P2

Version History	
June 2020	Version 1.0

Dependencies	- BIA.3: Data Lifecycle Management

Domain Name	Business Intelligence and Analytics	Domain ID	BIA

Control Name	Artifacts	Control ID	BIA.5
Control Description	As part of the Artifacts control, the Entity shall document in a register its BI and Analytics Use Cases		

Specification #	Specification Name	Control Specification	Priority
BIA.5.1	Business Intelligence and Analytics Register	The Entity shall document in a register its BI and Analytics Use Cases, final review of outcomes delivered as a result of each implementation and related process documentation whereby read access is granted to all Entity stakeholders.	P3

Version History	
June 2020	Version 1.0

Dependencies	- BIA.3: Data Lifecycle Management

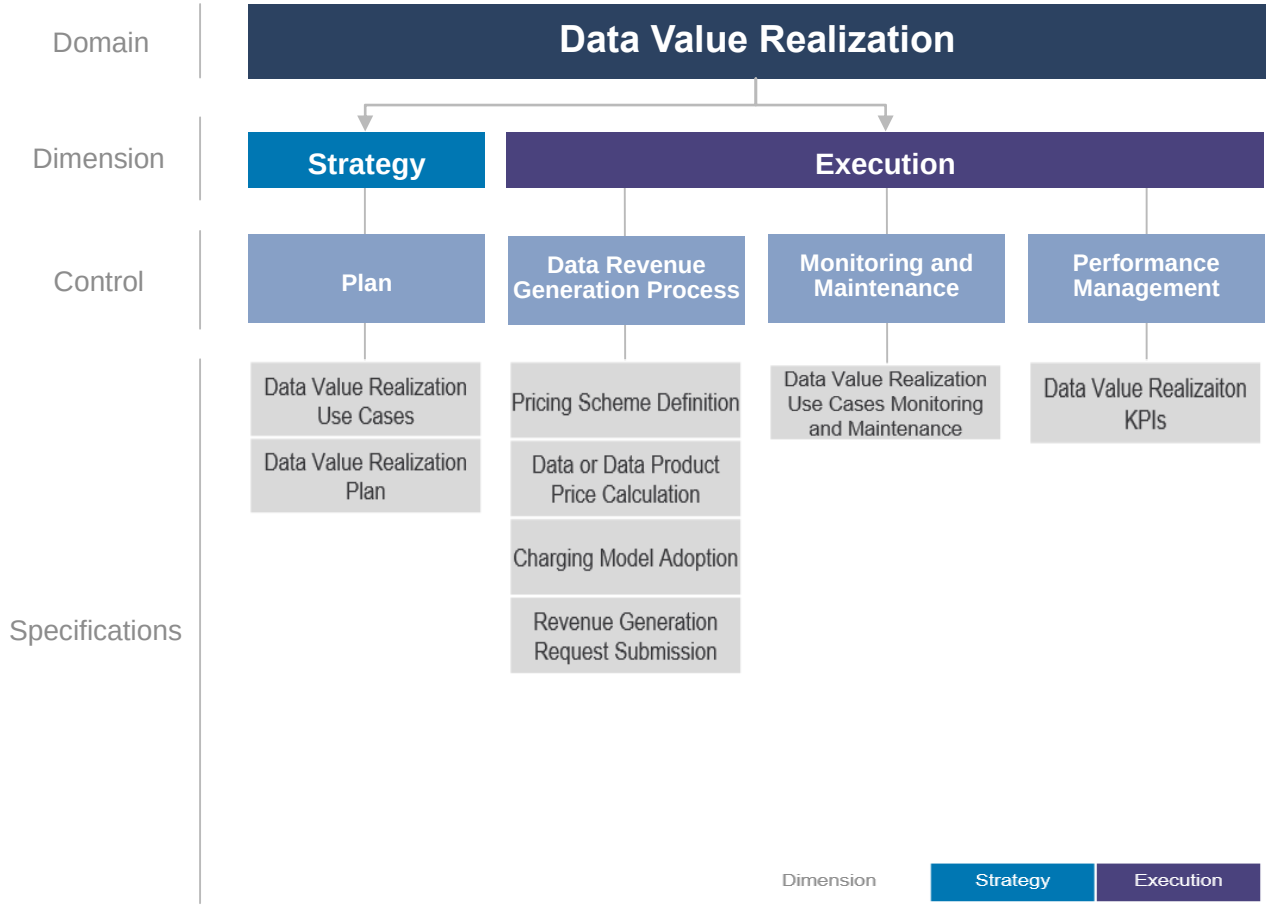
9.9.3. References

Business Intelligence and Analytics Domain References	- DAMA DMBOK 2nd Edition (Mosley and Brackett, 2017) - Data Management for Advanced Analytics (TDWI Report, 2019) - Leading Trends In Data Analytics (TDWI, 2019) - How to Create Data and Analytics Everywhere for Everyone: Top Insights for Digital Business (Gartner, 2019) - Data & Analytics Playbook (Accenture, 2019)

9.10. Data Value Realization Domain

9.10.1. Domain on a Page

Data Value Realization domain comprises of 4 controls and 8 specifications. This domain involves the continuous evaluation of data assets for potential data driven use cases that generate revenue or reduce operating costs for the organization.



9.10.2. Controls and Specifications

Domain Name	Data Value Realization	Domain ID	DVR

Control Name	Plan	Control ID	DVR.1
Control Description	As part of the Plan control, the Entity shall identify and document Data Value Realization Use Cases and create a Data Value Realization Plan		

Specification #	Specification Name	Control Specification	Priority
DVR.1.1	Data Value Realization Use Cases	The Entity shall identify, and document Data Value Realization Use Cases. The Data Value Realization Use Cases shall include, at minimum, the following: 1. Data Revenue Generation Use Cases - Data or Data Products to generate revenue from, as defined in the Data Revenue Framework Regulation. Data or Data Products are the outputs resulting from transforming data for added value by performing additional data collection, enrichment, preparation, analysis, or presentation 2. Cost Saving Use Cases – Data-driven use cases that will contribute directly or indirectly to reducing costs and achieving efficiencies by leveraging data to improve organizational operational performance, productivity, and products and services. For each Data Value Realization Use Case the Entity shall estimate and document the projected Payback period and Return on Investment (ROI).	P1
DVR.1.2	Data Value Realization Plan	Based on the Entity's defined Data Management and Personal Data Protection Strategy and Plan, the Entity shall create a Data Value Realization Plan to realize its data revenue generation potential and drive data-related cost optimization initiatives. The plan shall include, at minimum, the following: 1. Roadmap with the activities and key milestones for the implementation of Data	P1

		Value Realization Use Cases. The activities shall, at minimum, incorporate what is needed to achieve the specifications in this domain 2. Assignment of the required resources and budget to manage the implementation of Data Value Realization Use Cases.	

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan**

Domain Name	Data Value Realization	Domain ID	DVR

Control Name	Data Revenue Generation Process	Control ID	DVR.2
Control Description	As part of the Data Revenue Generation Process, the Entity shall for each Data or Data product expecting to generate revenue from select an appropriate Pricing Scheme Model, calculate and document the Total Cost, define and document the adopted Charging Model after reviewing it from Chef Data Office, and submit a revenue generation request		

Specification #	Specification Name	Control Specification	Priority
DVR.2.1	Pricing Scheme Definition	The Entity shall, for each Data or Data Product expecting to generate revenue from, select and document an appropriate Pricing Scheme Model based on the scenarios outlined in the Data Revenue Framework Regulation.	P2
DVR.2.2	Data or Data Product Price Calculation	The Entity shall, for each Data or Data Product expecting to generate revenue from, calculate and document the Total Cost as defined by the Data Revenue Framework Regulation. The total cost shall include, at minimum, the following: 1. Data Collection Cost - Cost incurred for collecting, cleansing, and curating data 2. Data Development Cost - Cost incurred for developing analytical models, data visualizations and other value-added services provided on top of collected data.	P2
DVR.2.3	Charging Model Adoption	The Entity shall for each Data or Data Product that it is expecting to generate revenue from, define and document the adopted Charging Model. The Entity shall choose, at minimum, from the following Charging Models defined in the Data Revenue Framework Regulation: 1. Subscription Model 2. Consumption-Based Model 3. Freemium / Premium Model 4. One-Time Fee Model.	P2

DVR.2.4	**Revenue Generation Request Submission**	The Entity shall for each Data or Data Product that it is expecting to generate revenue from, submit a revenue generation request to the National Data Management Office. The request shall include, at minimum, the following: 1. Description of Data or Data Product 2. Pricing Scheme Documentation 3. Proposed Charging Model 4. Proposed Final Unit Price 5. Justification if the Final Unit Price does not follow the Cost Recovery Pricing Scheme.	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **DVR.1: Plan** - **DCL.3: Classification Process**

Domain Name	Data Value Realization	Domain ID	DVR

Control Name	Monitoring and Maintenance	Control ID	DVR.3
Control Description	As part of the Monitoring and Maintenance control, the Entity shall actively monitor and maintain implemented Data Value Realization Use Cases		

Specification #	Specification Name	Control Specification	Priority
DVR.3.1	Data Value Realization Use Cases Monitoring and Maintenance	"The Entity shall actively monitor and maintain implemented Data Value Realization Use Cases. The monitoring and maintenance shall include, at minimum, the following: 1. Measuring and validating KPIs (ROI and Payback Period) against projected values in the Data Value Realization Plan 2. Developing Change Request documents to accommodate change requirements from end users 3. Reporting defects or malfunctions in the use case implemented.	P3

Version History	
June 2020	Version 1.0

Dependencies	- DVR.2: Data Revenue Generation Process

Domain Name	Data Value Realization	Domain ID	DVR

Control Name	Performance Management	Control ID	DVR.4
Control Description	As part of the Performance Management control, the Entity establish key performance indicators (KPIs) to measure the Entity's Data Value Realization activities		

Specification #	Specification Name	Control Specification	Priority
DVR.4.1	Data Value Realization KPIs	The Entity shall establish key performance indicators (KPIs) to measure the Entity's Data Value Realization activities. KPIs shall include, at minimum, the following: 1. Number of Data Products developed 2. Number of Data or Data Products revenue generation requests raised to NDMO 3. Number of Data Products that generated revenue 4. Total revenue generated from offering Data or Data Products 5. Total cost saved from implemented Cost Saving Use Cases 6. Data Value Realization Use Case Payback period 7. Data Value Realization Use Case Return on Investment (ROI).	P2

Version History	
June 2020	Version 1.0

Dependencies	- DVR.2: Data Revenue Generation Process

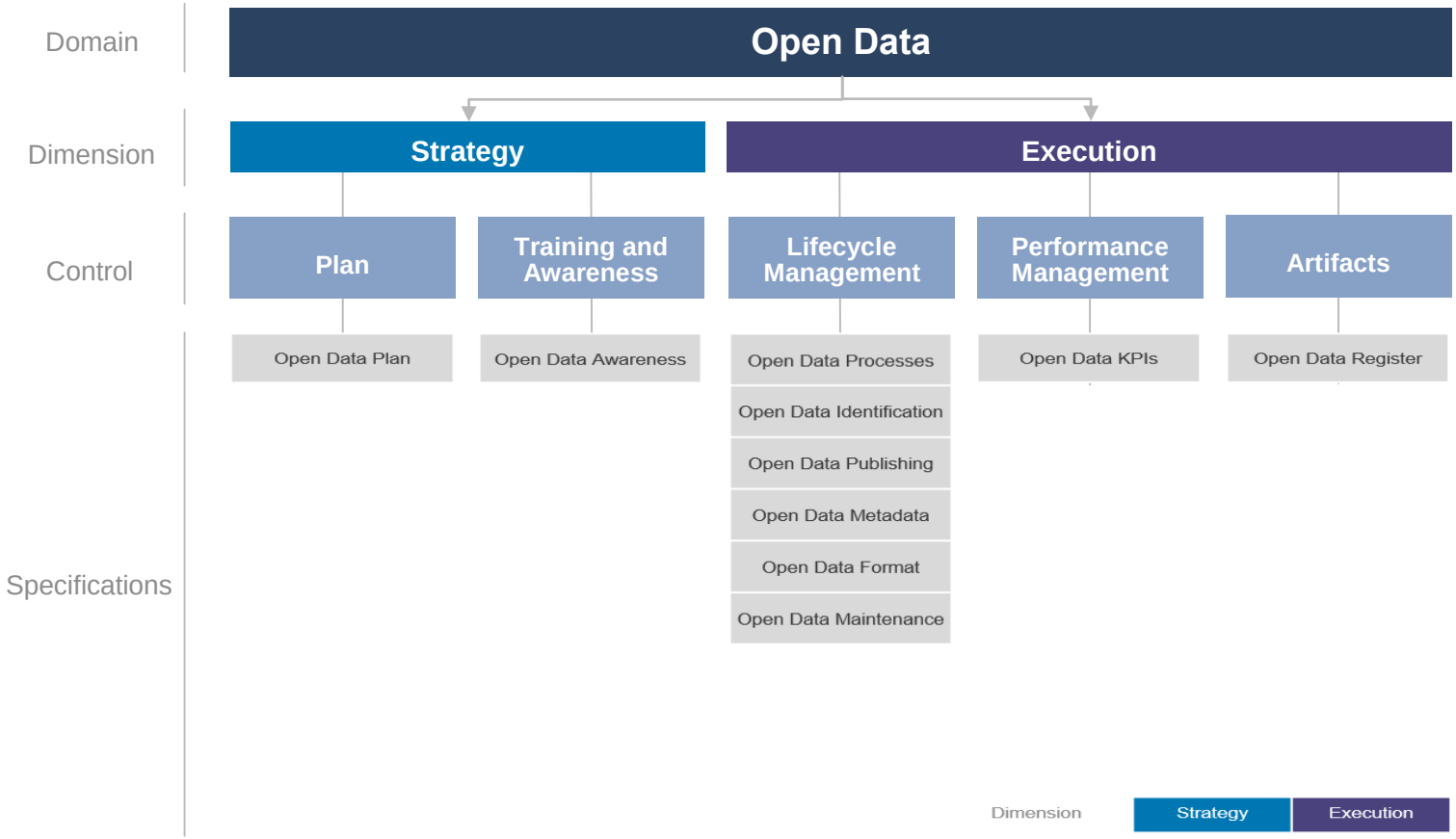
9.10.3. References

Data Value Realization Domain References	- National Data Management Office's Data Revenue Framework Regulation - National Data Management Office's Data Classification Regulation - National Data Management Office's Data Sharing Regulation

9.11. Open Data Domain

9.11.1. Domain on a Page

Open Data domain comprises of 5 controls and 10 specifications. This domain focuses on the organization’s data which could be made available for public consumption to enhance transparency, accelerate innovation, and foster economic growth.



9.11.2. Controls and Specifications

Domain Name	Open Data	Domain ID	OD

Control Name	Plan	Control ID	OD.1
Control Description	As part of the Plan control, the Entity shall develop an Open Data Plan		

Specification #	Specification Name	Control Specification	Priority
OD.1.1	Open Data Plan	Based on the Entity's defined Data Management and Personal Data Protection Strategy and Plan, the Entity shall create an Open Data Plan to identify and coordinate the publishing of its Open Datasets. The plan shall include, at minimum, the following: 1. Roadmap with the activities and key milestones for the implementation of Open Data initiatives. The activities shall, at minimum, incorporate what is needed to achieve the specifications in this domain 2. Assignment of the required resources and budget to manage the implementation of Open Data initiatives.	P1

Version History	
June 2020	Version 1.0

Dependencies	- DG.1: Strategy and Plan

Domain Name	Open Data	Domain ID	OD

Control Name	Training and Awareness	Control ID	OD.2
Control Description	As part of the Training and Awareness control, the Entity shall plan awareness campaigns to promote the usage and benefits of Open Data		

Specification #	Specification Name	Control Specification	Priority
OD.2.1	Open Data Awareness	The Entity shall plan awareness campaigns to ensure potential users are aware of the existence, nature, and quality of the Open Data offered by the Entity. The awareness plan shall include, at minimum, the following: 1. Usage of Open Data and its various positive social and economic benefits 2. Promoting the Entity Open Data and related activities	P2

Version History	
June 2020	Version 1.0

Dependencies	- OD.1: Plan

Domain Name	Open Data	Domain ID	OD

Control Name	Data Lifecycle Management	Control ID	OD.3
Control Description	As part of the Data Lifecycle Management control, the Entity shall identify, publish and maintain its Open Datasets		

Specification #	Specification Name	Control Specification	Priority
OD.3.1	Open Data Processes	The Entity shall, in alignment to the National Data Management Office's Open Data Regulation, develop and document processes required across the lifecycle of Open Data, including, at minimum, the following: 1. Processes to identify public datasets to be published the Entity 2. 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 restricted data 3. Processes for gathering feedback, analyzing performance at the Entity level, and improving the overall Open Data national impact.	P1
OD.3.2	Open Data Identification	The Entity shall, as part of the identification process: 1. Identify and document all data classified as 'public' and prioritize each dataset identified as Open Data 2. Perform a valuation of the identified dataset to drive decision making on whether it should be published as open data or not 3. Assess whether some combination of any publicly available data and the data intended to be published could allow for the unauthorized disclosure of personal information or create any other security or privacy risk or threat	P1

		Refer to the National Data Management Office's Open Data Regulation for detailed requirements	
OD.3.3	**Open Data Publishing**	The Entity shall publish datasets identified under the KSA Open Data License, as referred to in the National Data Management Office's Open Data Regulation	P1
OD.3.4	**Open Data Metadata**	The Entity shall identify and document the metadata necessary within the Open Dataset to easily identify, describe and search for it once published	P2
OD.3.5	**Open Data Format**	The Entity shall use standardized formats when publishing its datasets that are, at minimum, in machine-readable form. Common formats that meet this standard include, but may not be limited to, the following: 1. CSV - Comma Separated Values 2. JSON - JavaScript Object Notation 3. XML - eXtensible Markup Language 4. RDF - Resource Description Framework. The Entity shall also accompany datasets with documentation containing instructions on how to use them in relation to its published format	P1
OD.3.6	**Open Data Maintenance**	The Entity shall, as part of the maintenance process: 1. Regularly update and document changes to its published Open Datasets and associated metadata whenever changes occur 2. Perform continuous review of the published Open Datasets to ensure they meet defined regulatory requirements Maintain data traceability by documenting data provenance and maintaining versioning history of the dataset	P3

Version History	
June 2020	**Version 1.0**

Dependencies	- **OD.1: Plan** - **DC.3: Classification Process** - **DG.4: Data Management and Personal Data Protection Organization**

Domain Name	Open Data	Domain ID	OD

Control Name	Performance Management	Control ID	OD.4
Control Description	As part of the Performance Management control, the Entity shall establish Key Performance indicators (KPIs) to measure the progress of the Open Data Plan		

Specification #	Specification Name	Control Specification	Priority
OD.4.1	Open Data KPIs	The Entity shall establish key performance indicators (KPIs) to measure the progress of the Open Data Plan and gather statistics on the published Open Datasets. KPIs shall include, at minimum, the following: 1. Number of downloads per published Open Dataset 2. Number of identified and prioritized Open Datasets 3. Number of identified Open Datasets that have been published 4. Number of updates performed on published Open Datasets.	P2

Version History	
June 2020	Version 1.0

Dependencies	- OD.3: Data Lifecycle Management

Domain Name	Open Data	Domain ID	OD

Control Name	Artifacts	Control ID	OD.5
Control Description	As part of the Artifacts control, the Entity document in a register the list of all Open Datasets		

Specification #	Specification Name	Control Specification	Priority
OD.5.1	Open Data Register	The Entity shall document in a register the list of all its identified Open Datasets combined with a log of open data activities conducted and decisions taken during the Data Lifecycle Management process	P2

Version History	
June 2020	Version 1.0

Dependencies	- OD.3: Data Lifecycle Management

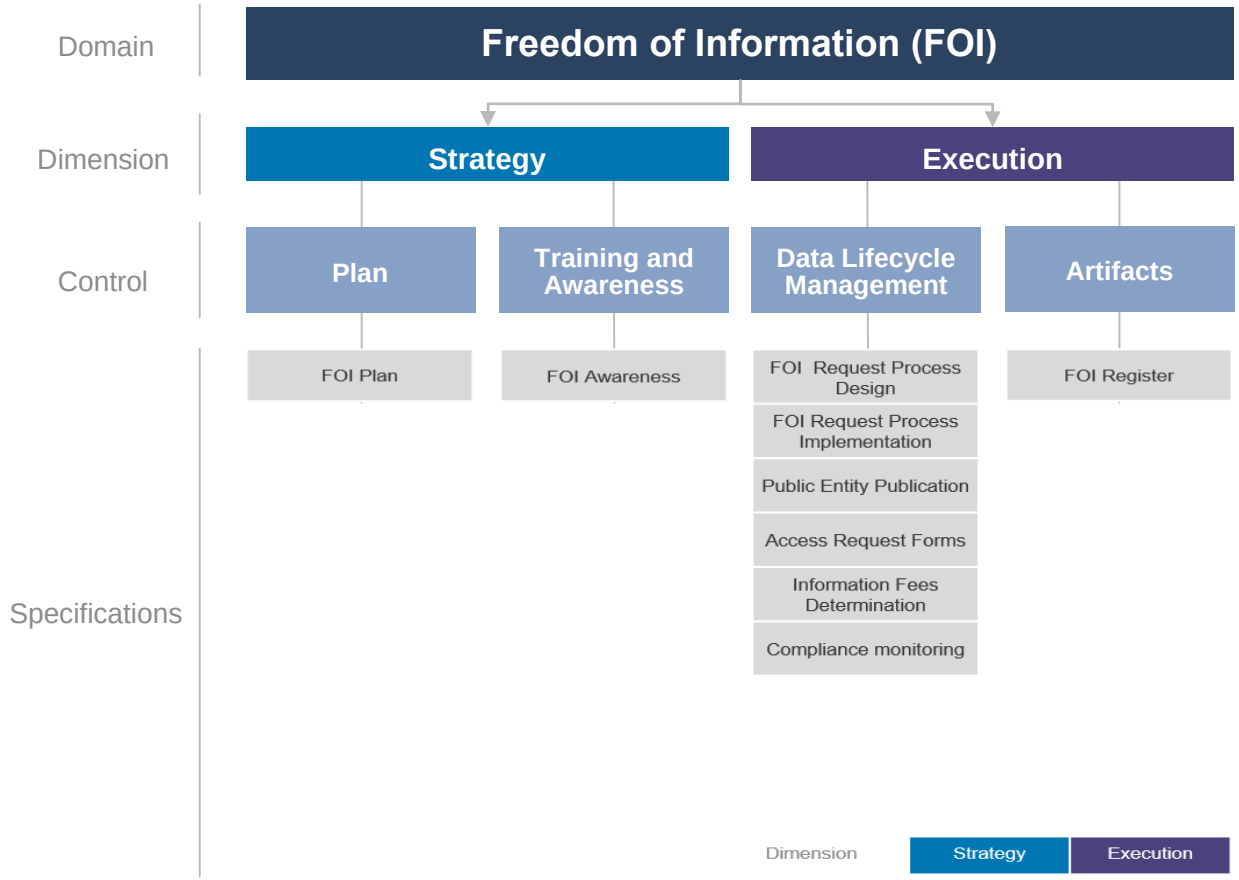
9.11.3. References

Open Data Domain References	- Open Data Charter - National Data Management Office's Open Data Regulation - National Data Management Office's Data Classification Regulation

9.12. Freedom of Information Domain

9.12.1. Domain on a Page

Freedom of Information domain comprises of 4 controls and 9 specifications. This domain focuses on providing Saudi citizens access to government information, portraying the process for accessing such information, and the appeal mechanism in the event of a dispute.



9.12.2. Controls and Specifications

Domain Name	Freedom of Information	Domain ID	FOI

Control Name	Plan	Control ID	FOI.1
Control Description	As part of the Plan control, the Entity shall develop a Freedom of Information Plan to address both strategic and operational requirements of the National Data Management Office's Freedom of Information Regulations		

Specification #	Specification Name	Control Specification	Priority
FOI.1.1	FOI Plan	Based on the Entity's defined Data Management and Personal Data Protection Strategy and Plan, the Entity shall create a Freedom of Information Plan to address both strategic and operational requirements of the National Data Management Office's Freedom of Information Regulations. The plan shall include, at minimum, the following: 1. Roadmap with the activities and key milestones for achieving and maintaining the Entity's compliance with the National Data Management Office's Freedom of Information Regulations. The activities shall, at minimum, incorporate what is needed to achieve the specifications in this domain 2. Assignment of the required resources and budget to achieve and maintain the Entity's compliance with the National Data Management Office's Freedom of Information Regulations.	P1

Version History	
June 2020	Version 1.0

Dependencies	- DG.1: Strategy and Plan

Domain Name	Freedom of Information	Domain ID	FOI

Control Name	Training and Awareness	Control ID	FOI.2
Control Description	As part of the Training and Awareness control, the Entity shall launch awareness campaigns to promote and enhance the culture of transparency and raise awareness of the National Data Management Office's Freedom of Information Regulations		

Specification #	Specification Name	Control Specification	Priority
FOI.2.1	FOI Awareness	The Entity shall launch awareness campaigns to promote and enhance the culture of transparency and to raise awareness of the National Data Management Office's Freedom of Information Regulations and right to access Public Information. The awareness campaigns shall include, at minimum, the following: 1. Raising awareness across the employees involved in the processing of FOI Access Requests to understand the main obligations and requirements of National Data Management Office's Freedom of Information Regulations 2. Raising awareness of the Freedom of Information Principles and their applicability on Saudi citizens' rights.	P2

Version History	
June 2020	Version 1.0

Dependencies	- FOI.1: Plan

Domain Name	Freedom of Information	Domain ID	FOI

Control Name	Data Lifecycle Management	Control ID	FOI.3
Control Description	As part of the Data Lifecycle Management control, the Entity shall design and implement a request process, publish Public Entity Publication, prepare request forms, determine request fees, and monitor compliance		

Specification #	Specification Name	Control Specification	Priority
FOI.3.1	FOI Request Process Design	The Entity shall design and document a standardized Request for Information Process and develop the procedures to manage, process and document the requests to access Public Information according to in the National Data Management Office Freedom of Information Regulations.	P1
FOI.3.2	FOI Request Process Implementation	The Entity shall establish and follow a clear process to manage the requests to access Public Information according to the conditions and requirements defined in the National Data Management Office's Freedom of Information Regulation. As part of the process the Entity shall make one of the following decisions after receiving the request for access to Public Information within the period defined in the National Data Management Office's Freedom of Information Regulations: 1. Grant the access to Public Information 2. Deny the request to access Public Information 3. Extend the time required to provide a response to the Requestor 4. Notify the Requestor if the required information is available on the Entity's website or is not within its competence.	P1

FOI.3.3	**Public Entity Publication**	The Entity, under the National Data Management Office's Freedom of Information Regulation, shall publish on their official Government websites or its affiliate's websites, at minimum, the following information: 1. Laws, regulations, instructions and regulatory decisions applicable to the Entity 2. Entity's services provided and description detailing how to obtain access to those services 3. Entity's organizational structure including Entity's roles and responsibilities 4. Entity's job vacancy information, except information of security or military job vacancies as determined by security or military regulatory authorities or KSA Regulations 5. Entity's annual key strategic and operational reports including the Entity's financial statement 6. Entity's general statistics and updates on its activities including, at minimum, the following: 6a. Number of the Entity's employees 6b. Year of the Entity's establishment 6c. Number of the Entity's services provided in the last year 6d. Up-to-date Entity's activities' descriptions 7. Contact details to persons with valid licenses granted by the Entity including, at minimum, the following: 7a. Names of the persons 7b. Postal addresses of the person 7c. E-mail addresses of the persons 8. Information on projects offered or awarded by the Entity as prescribed by the Freedom of Information Regulations in respect of a risk that may affect people' life, health or property. The information shall include, at minimum, the following: 8a. Names of recipients 8b. Execution period	P3

		8c. Technical analysis 9. Guidelines and leaflets that raise the people's awareness of their Freedom of Information rights toward the Entity. If the information above is not applicable or available, the Entity shall provide a justification to the National Data Management Office.	
FOI.3.4	**Access Request Forms**	The Entity shall prepare request forms for access to Public Information - whether paper or electronic - specifying the required information to be provided by the Requestor. The required information shall include, at minimum, the following: 1. Information about the Requestor including name, address, national ID 2. Description of Public Information being requested 3. Purpose behind the request for access to public information 4. Legal basis for the request 5. Notice delivery method to the requestor (e-mail, national address) 6. Date of the request.	P1
FOI.3.5	**Information Fees Determination**	The Entity shall, for each granted Public Information Access Request, calculate and document a processing fee by adopting a Pricing Scheme as defined in the National Data Management Office's Data Value Realization Regulation.	P2

FOI.3.6	**Compliance monitoring**	The Entity shall conduct internal audits to monitor compliance with the National Data Management Office's Freedom of Information Regulations and document its findings in a report submitted to the Open Data and Information Access Officer. In cases of non-compliance, corrective actions should be taken with a notification to the Regulatory Authority and the National Data Management Office and documented within the audit findings report. Refer to the National Data Management Office's Freedom of Information Regulations for more detailed requirements.	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **FOI.1: Plan** - **DG.4: Data Management & Privacy Organization**

Domain Name	Freedom of Information	Domain ID	FOI

Control Name	Artifacts	Control ID	FOI.4
Control Description	As part of the Artifacts control, the Entity document in a register compliance records required by the National Data Management Office's Freedom of Information Regulations		

Specification #	Specification Name	Control Specification	Priority
FOI.4.1	FOI Register	The Entity shall document in a register compliance records as required by the National Data Management Office's Freedom of Information Regulations. The register shall include, at minimum, the following: 1. Information on the current Open Data and Information Access Officer 2. Public Information Access Requests Records 3. Public Entity Publication 4. Any other records, including the manner and format, that is required by the National Data Management Office's Freedom of Information Regulation. Refer to the National Data Management Office's Freedom of Information Regulations for more detailed requirements.	P3

Version History	
June 2020	Version 1.0

Dependencies	- FOI.3: Data Lifecycle Management

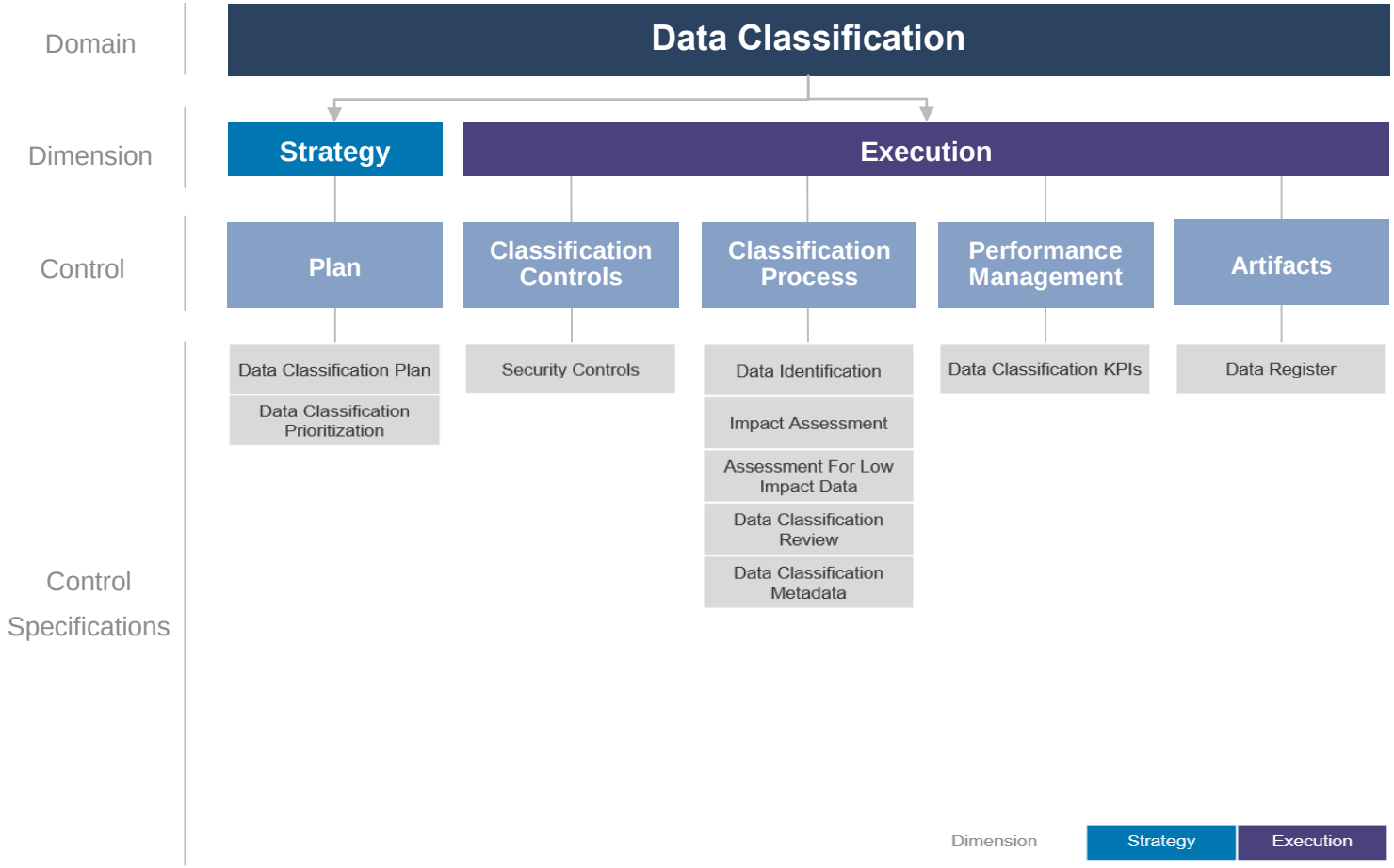
9.12.3. References

Freedom of Information Domain References	- National Data Management Office Freedom of Information Regulation

9.13. Data Classification Domain

9.13.1. Domain on a Page

Data Classification domain comprises of 5 controls and 10 specifications. This domain involves the categorization of data so that it may be used and protected efficiently. Data Classification levels are assigned following an impact assessment determining the potential damages caused by the mishandling of data or unauthorized access to data.



9.13.2. Controls and Specifications

Domain Name	Data Classification	Domain ID	DC

Control Name	Plan	Control ID	DC.1
Control Description	As part of the Plan control, the Entity shall develop a Data Classification Plan and prioritize its datasets and artifacts		

Specification #	Specification Name	Control Specification	Priority
DC.1.1	Data Classification Plan	Based on the Entity's defined Data Management and Personal Data Protection Strategy and Plan, the Entity shall create a Data Classification Plan to manage and orchestrate its Data Classification activities. The plan shall include, at minimum, the following: 1. Roadmap with the activities and key milestones for the classification of Entity's data. The activities shall, at minimum, incorporate what is needed to achieve the specifications in this domain 2. Assignment of the required resources and budget to manage the classification of Entity's data.	P1
DC.1.2	Data Classification Prioritization	The Entity shall prioritize the Entity's datasets and artifacts to be classified. The result of the prioritization shall be a list of ranked datasets and artifacts to be followed when establishing an order of the Entity's Data Classification.	P1

Version History	
June 2020	Version 1.0

Dependencies	- DG.1: Strategy and Plan

Domain Name	Data Classification	Domain ID	DC

Control Name	Classification Controls	Control ID	DC.2
Control Description	As part of the Classification Controls, the Entity shall assign data handling and protection controls to datasets and artifacts		

Specification #	Specification Name	Control Specification	Priority
DC.2.1	Security Controls	The Entity shall assign data handling and protection controls to datasets and artifacts based on their classification to ensure secure handling, processing, sharing and disposal of data by following the National Cybersecurity Authority regulations.	*As specified by NCA*

Version History	
June 2020	Version 1.0

Dependencies	- DC.3: Classification Process

Domain Name	Data Classification	Domain ID	DC

Control Name	Classification Process	Control ID	DC.3
Control Description	As part of the Classification Process control, the Entity shall identify all datasets and artifacts owned by the Entity, conduct for them impact assessment of the potential damages and review assigned data classification levels		

Specification #	Specification Name	Control Specification	Priority
DC.3.1	Data Identification	The Entity shall identify and inventory all datasets and artifacts owned by the Entity as part of the Data Classification Implementation process detailed in the National Data Management Office's Data Classification Regulation. If the Entity had already implemented its Data Catalog automated tool, the Entity shall use it to inventory all its datasets and artifacts.	P1
DC.3.2	Impact Assessment	The Entity shall conduct an impact assessment of the potential damages due to an unauthorized access to all its identified datasets and artifacts. The impact assessment shall include the following steps: 1. Identification of the potential categories impacted amongst national interest, organizations, individuals and environment 2. Selection of the level of impact of potential damage for the identified categories amongst 'High', 'Medium', 'Low' and 'None/Insignificant' 3. Assignment of classification levels to datasets and artifacts based on the selected impact level: 3a. If the impact level was assessed as 'High', then datasets and artifacts shall be classified as 'Top Secret' 3b. If the impact level was assessed as 'Medium', then datasets and artifacts shall be classified as 'Secret'	P1

		3c. If the impact level was assessed as 'Low', then datasets and artifacts shall be classified as 'Confidential' 3d. If the impact level was assessed as 'None/Insignificant', then datasets and artifacts shall be classified as 'Public'. The assessment shall be conducted as a part of the Data Classification Implementation process by following the National Data Management Office's Data Classification Regulation.	
DC.3.3	**Assessment for Low Impact Data**	The Entity shall assess the possibility to Classify 'Low' impact data as 'Public' instead of 'Confidential'. The assessment shall include the following: 1. Evaluation if the disclosure of 'Low' impact data is in breach of any existing regulation 2. Identify the potential benefits of opening such datasets and artifacts and consider whether those would outweigh the negative impacts If release of 'Low' impact data is not in breach of any existing regulation and if benefits of release outweigh the negative impact, the Entity shall classify 'Low' impact data as 'Public'. The assessment shall be conducted as part of the Data Classification Implementation process by following the National Data Management Office's Data Classification Regulation.	P1
DC.3.4	**Data Classification Review**	The Entity shall review all its classified datasets and artifacts to ensure that the classification levels assigned to them are the most appropriate ones as part of the Data Classification Implementation process by following National Data Management Office's Data Classification Regulation.	P2
DC.3.5	**Data Classification Metadata**	The Entity shall publish classification levels assigned to its datasets and artifacts as the metadata registered within the Data Catalog automated tool. The population of the metadata shall be executed according to the	P2

		process defined in Metadata and Data Catalog Management domain.	

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan** - **DG.4: Data Management and Personal Data Protection Organization** - **DC.1: Plan**

Domain Name	Data Classification	Domain ID	DC

Control Name	Performance Management	Control ID	DC.4
Control Description	As part of the Performance Management control, the Entity shall establish key performance indicators (KPIs) to measure the progress on the classification plan and implementation of the Entity's Data Classification process		

Specification #	Specification Name	Control Specification	Priority
DC.4.1	Data Classification KPIs	The Entity shall establish key performance indicators (KPIs) to measure the progress on the classification plan and the implementation of the Entity's Data Classification process. KPIs shall include, at minimum, the following: 1. % of datasets and artifacts classified 2. % of datasets and artifacts classified by a classification level 3. % of 'Low' impact data classified as 'Confidential' 4. % of classified datasets and artifacts that has been reviewed and approved.	P2

Version History	
June 2020	Version 1.0

Dependencies	- DC.3: Classification Process

Domain Name	Data Classification	Domain ID	DC

Control Name	Artifacts	Control ID	DC.5
Control Description	As part of the Artifacts control, the Entity document in a register the list of all its identified datasets and artifacts combined with log of Data Classification activities		

Specification #	Specification Name	Control Specification	Priority
DC.5.1	Data Register	The Entity shall document in a register the list of all its identified datasets and artifacts combined with log of Data Classification activities conducted during Data Classification Implementation process. The register shall include, at minimum, the following: 1. List of the Entity's identified datasets and artifacts 2. Classification levels assigned to identified datasets and artifacts 3. Dates of assignment of classification levels to identified datasets and artifacts 4. Classification duration applied to identified datasets and artifacts 5. Classification levels approved during review 6. Dates of classification levels' review.	P2

Version History	
June 2020	Version 1.0

Dependencies	- DC.3: Classification Process

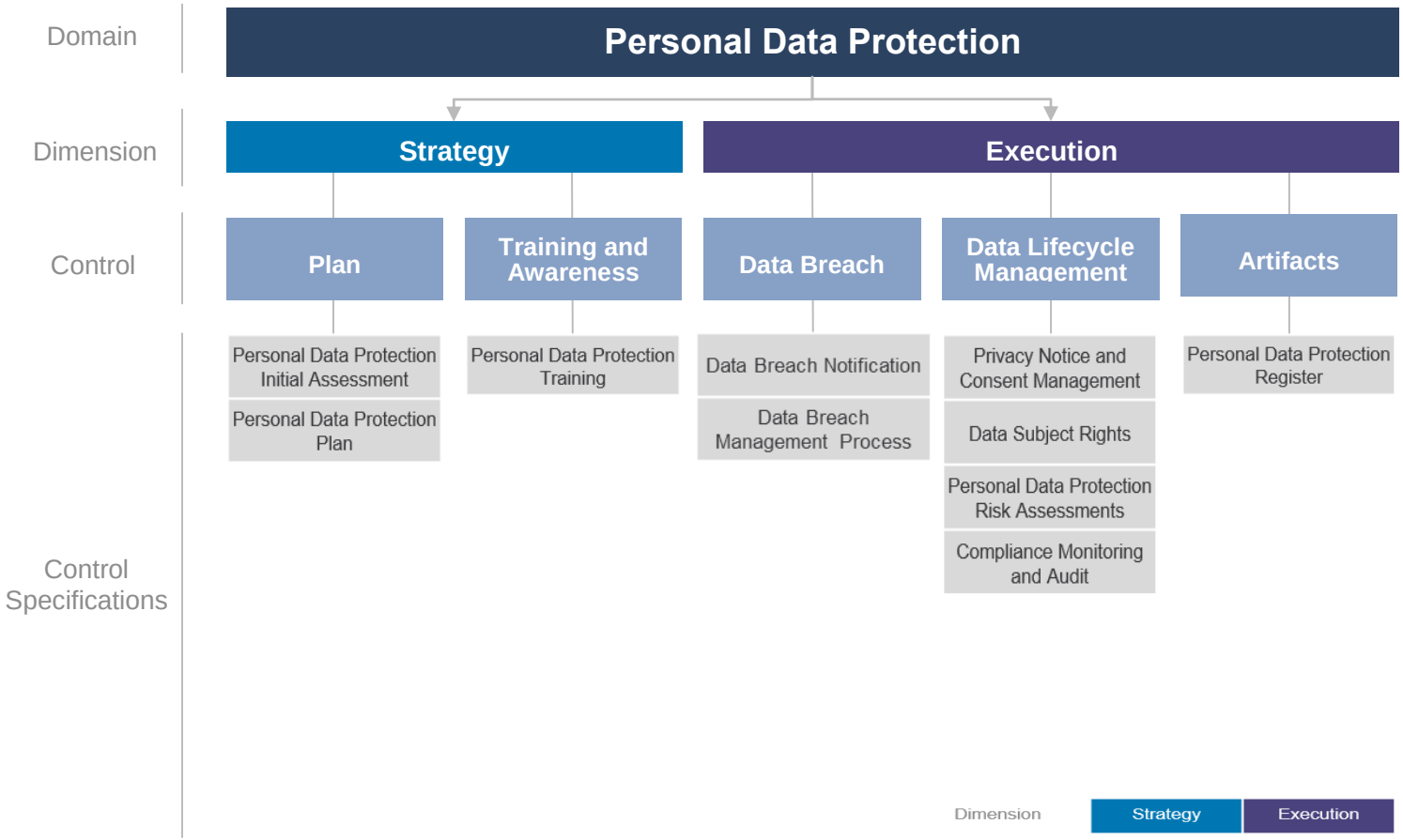
9.13.3. References

Data Classification Domain References	- National Data Management Office Data Classification Regulation - ISO 27001

9.14. Personal Data Protection Domain

9.14.1. Domain on a Page

Personal Data Protection domain comprises of 5 controls and 10 specifications. This domain focuses on protection of a subject's entitlement to the proper handling and non-disclosure of their personal information.



9.14.2. Controls and Specifications

Domain Name	Personal Data Protection	Domain ID	PDP

Control Name	Plan	Control ID	PDP.1
Control Description	As part of the Plan control, the Entity shall conduct an Initial Personal Data Protection Assessment and establish a Personal Data Protection Plan to address privacy strategic and operational requirements		

Specification #	Specification Name	Control Specification	Priority
PDP.1.1	Personal Data Protection Initial Assessment	The Entity shall perform an initial Personal Data Protection Assessment to evaluate the current state of the Personal Data Protection environment. The assessment shall include, at minimum, the following: 1. Identification of types of personal data being collected 2. Location and method of storage of personal data 3. Current processing and uses of the personal data 4. Privacy challenges to meet compliance with the National Data Management Office's Personal Data Protection Regulations.	P1
PDP.1.2	Personal Data Protection Plan	Based on the Entity's defined Data Management and Personal Data Protection Strategy and Plan, the Entity shall create a Personal Data Protection Plan to address both the strategic and operational privacy requirements of the National Data Management Office's Personal Data Protection Regulations. The plan shall include, at minimum, the following: 1. Roadmap with the activities and key milestones for achieving and maintaining the Entity's compliance with the National Data Management Office's Personal Data Protection Regulations. The activities shall,	P1

		at minimum, incorporate what is needed to achieve the specifications in this domain 2. Assignment of the required resources and budget to achieve and maintain the Entity's compliance with the National Data Management Office's Personal Data Protection Regulations.	

Version History	
June 2020	**Version 1.0**

Dependencies	- **DG.1: Strategy and Plan**

Domain Name	Personal Data Protection	Domain ID	PDP

Control Name	Training and Awareness	Control ID	PDP.2
Control Description	As part of the Training and Awareness control, the Entity shall conduct a Personal Data Protection training to promote a Personal Data Protection-centric culture		

Specification #	Specification Name	Control Specification	Priority
PDP.2.1	Personal Data Protection Training	The Entity shall conduct the Personal Data Protection training for every employee to promote a Personal Data Protection-centric culture in accordance with the Entity-specific and national privacy regulations. The training shall include, at minimum, the following: 1. Importance of Personal Data Protection and the Impacts and consequences to the Entity and / or Data Subject 2. Definition of Personal Data 3. Data Subject Data Rights 4. Entity and Data Subject Responsibilities 5. 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.	P1

Version History	
June 2020	Version 1.0

Dependencies	- PDP.1: Plan

Domain Name	Personal Data Protection	Domain ID	PDP

Control Name	Data Breach	Control ID	PDP.3
Control Description	As part of the Data Breach control, the Entity shall establish a Data Breach Process		

Specification #	Specification Name	Control Specification	Priority
PDP.3.1	Data Breach Notification	The Entity's Data Controller or Data Processor handling personal data shall, in the event it is determined that personal data has been compromised, notify the Regulatory Authority within the allotted timeframe specified within the National Data Management Office's Personal Data Protection Regulations. The allotted timeframe for notification is 72 hours. Refer to the National Data Management Office's Personal Data Protection Regulations for more detailed requirements.	P2
PDP.3.2	Data Breach Management Process	The Entity shall develop and document breach management procedures to directly manage and address the privacy violations and to set the functions and responsibilities for the affected work team, including cases in which the Regulatory Authority is notified once a breach has been identified. The breach management process shall include, at minimum, the following: 1. Conducting an incident review by the Data Controller with the Regulatory Authority 2. Formulating an immediate response to the incident by the Data Controller and / or Data Processor 3. Implementing the permanent corrective actions when issued by the Regulatory Authority 4. Conducting testing of the implemented corrective actions to validate personal data protection solution(s).	P1

		Refer to the National Data Management Office's Personal Data Protection Regulations, as well as NCA's guidance for more detailed requirements.	

Version History	
June 2020	**Version 1.0**

Dependencies	- **PDP.1: Plan**

Domain Name	Personal Data Protection	Domain ID	PDP

Control Name	Data Lifecycle Management	Control ID	PDP.4
Control Description	As part of the Data Lifecycle Management control, the Entity shall establish a Privacy Notice, Consent Management framework, its Data Subject Rights Processes, and conduct internal audits		

Specification #	Specification Name	Control Specification	Priority
PDP.4.1	Privacy Notice and Consent Management	The Entity shall establish, at minimum, the following Privacy Notice and Consent Management components: 1. Define and document its processes for providing Data Subjects with notice and requesting consent at all points along the data lifecycle where personal data is collected as prescribed by the National Data Management Office's Personal Data Protection Regulations 2. The Entity shall provide all possible options to Data Subject and his (implicit / explicit) approval shall be obtained regarding the collection, use or disclosure of personal data 3. The Entity shall document and make available a Privacy Notice for Data Subjects to review before or at the time the Entity requests permission to collect personal data 4. In the event the Data Controller maintains a presence on internet, a hyperlink to privacy notice must be maintained. The notice must be made available to the National Data Management Office for inspection upon request. Refer to the NMDO Personal Data Protection Regulations for more detailed requirements.	P2
PDP.4.2	Data Subject Rights	The Entity shall establish and document its Data Rights Management processes to support the rights of Data Subjects, in accordance with the National Data Management Office's Personal	P2

		Data Protection Regulations, whereby the Data Subject has a: 1. Right to be informed 2. Right to access 3. Right to rectification 4. Right to erasure 5. Right to object 6. Right to restrict processing 7. Right to data portability 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. Refer to the National Data Management Office's Personal Data Protection Regulations for more detailed requirements.	
PDP.4.3	**Personal Data Protection Risk Assessments**	The Entity shall conduct yearly risk assessments of the operation and use of its information systems containing personal data, including the collection and processing of personal data, and the storing and transmittal of personal data by each system - whether automated or manual. Risk assessment findings shall, at minimum, be: 1c. Documented 1d. Analyzed for impact and likelihood of occurrence 1e. Evaluated against current regulations obligations and criticality to resolve.	P3
PDP.4.4	**Compliance Monitoring and Audit**	The Entity shall conduct internal audits to monitor compliance with privacy regulations and document its findings in a report presented to the Data Protection Officer. In cases of non-compliance, corrective actions should be taken with a notification to the Regulatory Authority and the National Data Management Office and documented within the audit findings report. Refer to the National Data Management Office's Personal Data Protection Regulations for more detailed requirements.	P2

Version History	
June 2020	**Version 1.0**

Dependencies	- **PDP.1: Plan** - **PDP.3: Personal Data Protection Breach** - **DG.4: Data Management and Personal Data Protection Organization**

Domain Name	Personal Data Protection	Domain ID	PDP

Control Name	Artifacts	Control ID	PDP.5
Control Description	As part of the Artefacts control, the Entity shall document in a register its compliance records		

Specification #	Specification Name	Control Specification	Priority
PDP.5.1	Personal Data Protection Register	The Entity shall document in a register compliance records for a reasonable period of time, but not less than 24 months, and shall make those records available when requested by the National Data Management Office as defined in the National Data Management Office's Personal Data Protection Regulations. The register shall include, at minimum, a record of any collection and/or processing of any personal data.	P2

Version History	
June 2020	Version 1.0

Dependencies	- PDP.4: Data Lifecycle Management

9.14.3. References

Personal Data Protection Domain References	- National Data Management Office Personal Data Protection Regulation - The General Data Protection Regulation (2018) - California Consumer Privacy Act (2020**)**

9.15. Data Security and Protection Domain

Note: The National Cybersecurity Authority (NCA) is the government entity in charge of cybersecurity in Saudi Arabia. NCA serves as the national authority on this topic, both from a regulatory and operational perspective. Hence, the controls and corresponding specifications for the Data Security and Protection Domain will be detailed and addressed by NCA.

As part of the National Data Management and Personal Data Protection Standards addressed in this document, the framework provides a holistic view of the domains that are covered at a national level, one of which is the Data Security and Protection Domain.

As such, the Data Security controls highlighted below provide a viewpoint to entities of the Data Security topics that will be addressed by NCA. Compliance to the Data Security and Protection controls will be conducted by NCA, as per their requirements and methodology, and not as part of NDMO's annual Data Management and Personal Data Protection compliance assessment.

Below is an overview of these Data Security and Protection controls:

9.15.1. Controls

Domain Name	Data Security and Protection	Domain ID	DS

Control Name	Information Security Governance
Control Description	Establishing a plan to employ the tools, personnel and business processes to ensure security is carried out sufficiently to meet the Entity's needs for data protection

Control Name	Information Security Architecture
Control Description	The fundamental concepts and properties of the Entity's systems to enable the purpose, context and guidance for making security design decisions

Control Name	Information Systems Design, Development and Testing
Control Description	Minimum Security provisions to include as components into a system during its development, testing and implementation

Control Name	Identity and Access Management
Control Description	Identity of users and information systems requesting to have access to the Entity's information assets

Control Name	Third Party Supplier Security
Control Description	Obligations to ensure Information Security requirements are reflected in the Entity's engagement of third-party suppliers

Control Name	Information Security Training, Awareness and Communication
Control Description	Implementation of a comprehensive Information Security training program designed to introduce personnel the Entity's security expectations and obligations

Control Name	Information Asset Management
Control Description	Documented and maintained inventory of information assets containing critical Entity data

Control Name	Information Security Operations Management
Control Description	Operational duties by the Entity and its personnel to monitor, assess and protect the Entity's information assets

Control Name	Information Security Incident Management
Control Description	Operational processes established by the Entity for detecting, managing, recording and analyzing potential security threats and breaches as a result of monitoring its Operations

Control Name	Information Security Risk Management
Control Description	The identification, review, response and corrective actions to be employed by the Entity to prevent or mitigate risks for occurrence, consequences, impact and exposure to the Entity

Control Name	Information Systems Continuity Management
Control Description	A framework for preserving and maintaining the confidentiality, integrity and availability of data in the event of an incident (ISO 27001)

Version History	
June 2020	**Version 1.0**

9.15.2. References

Data Security Domain References	- Data Security Standards (PCI Security Standards Council, 2013) - ISO/IEC 27017 Cloud Security Standards (ISO, draft) - ISO/ISC 27018 Handling of Personally Identifiable Information (ISO, draft)