the dpsa

Department:
Public Service and Administration
REPUBLIC OF SOUTH AFRICA

PUBLIC SERVICE DATA GOVERNANCE FRAMEWORK

(Annexure A)

November 2024

CONTENT

1. PURPOSE

The purpose of this framework is to institutionalize control and authority ***(planning, monitoring and enforcement)*** over the management of data assets in the public service.

2. INTRODUCTION

Data is defined as the representation of facts, such as text, numbers, graphics, images, sound and video, but transforms into information when endowed with definition, format, timeframe and relevance. (DAMA, 2017:2). The value of data can also be expressed in economic terms requiring organizations to manage it effectively. Data Management is defined as "the development, execution, and supervision of plans, policies, programs, and practices that deliver, control, protect, and enhance the value of data and information assets throughout their lifecycles" (DAMA, 2017:17). A lifecycle management approach is followed when managing data and this includes processes and activities that create or obtain it (data), those that move, transform, and store it and enable it to be maintained and shared, and those that use or apply it, as well as those that dispose of it. Data is rarely static and throughout its lifecycle it may be cleansed, transformed, merged, enhanced, or aggregated. As data is used or enhanced, new data is often created highlighting internal iterations as part of lifecycle management. Below is a figure showing the diagrammatical representation of the data management lifecycle.

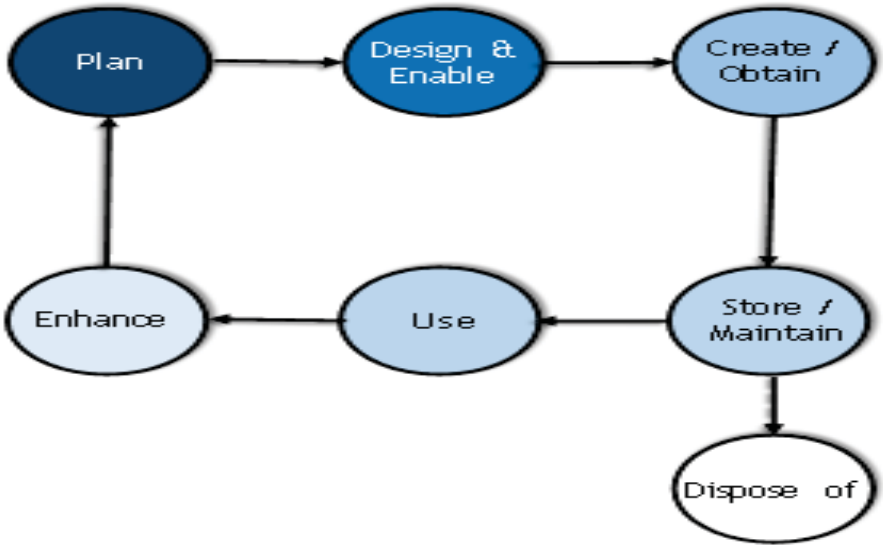


Figure1: Data Lifecycle Key Activities [DAMA DMBOK2: 2017,29]

Data management has three broad phases with each being made up of knowledge areas and these are:

- **The foundation phase**: *(data governance, data architecture, metadata and data quality management)*,
- **The lifecycle management phase:** *(data security, data modelling and design, data storage and operations, data integration and operability, reference and master data management, and document and content management)*
- **The oversight phase** *(data warehousing and business intelligence)*.

Data management activities straddle across the above-mentioned data management phases. When viewed collectively, these activities will allow the public service to use data to be able to:

- Monitor progress towards service delivery as well as developmental goals and targets.
- Identify gaps and challenges in policy implementation.
- Assess the impact and effectiveness of programs and interventions.
- Make informed decisions, priority-setting and resource allocation.
- Foster transparency and accountability concerning governance matters.

The above requires the public service to have the appropriate capabilities to benefit from its data estate.

2.1. DATA MANAGEMENT KNOWLEDGE AREAS

The body of knowledge and best practices in the field of data management suggest the prioritization of a data governance framework as the foundation for all data management activities and disciplines as shown in the figure below.

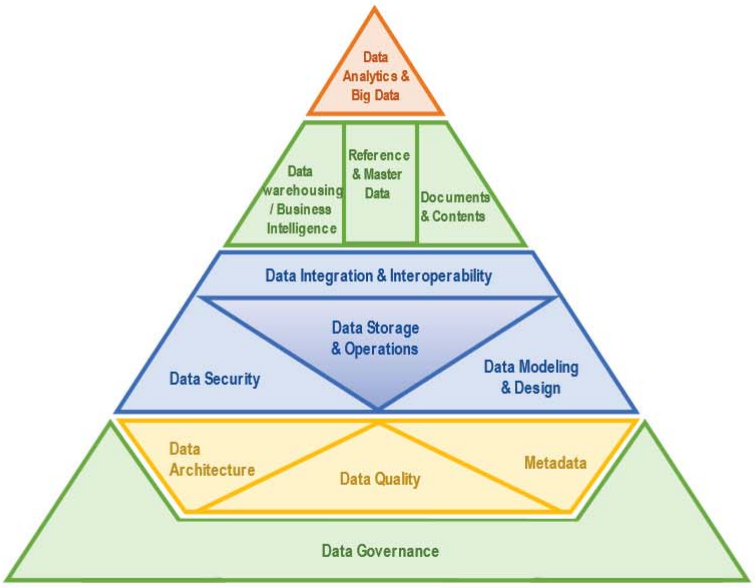


Figure 2: The Aiken Pyramid (DAMA DMBOK, 2017: 40)

- **Data governance**: It involves defining and implementing policies, standards, and processes to ensure the availability, usability, integrity, and security of data assets across the department. It encompasses roles and responsibilities, decision-making frameworks, and enforcement mechanisms to enable effective data stewardship and compliance.
- **Data architecture management**: It focuses on designing and maintaining the structure, integration, storage, and retrieval of data assets to meet business requirements. It involves defining data models, schemas, data flows, and storage mechanisms that support efficient data management and enable seamless data access and analysis

- **Data modelling and design:** It involves the processes and techniques for acquiring, creating, extracting, transforming, and loading data into departmental systems. It encompasses data profiling, cleansing, integration, and transformation activities to ensure data accuracy, consistency, and relevance for business purposes.
- **Data storage and operations:** It focuses on the day-to-day activities involved in

managing and maintaining data assets, including data storage, backup, recovery, and archival processes. It involves monitoring data quality, performance, and availability to ensure the reliability and integrity of data infrastructure and systems.

- **Data security**: It addresses the protection of data assets from unauthorized access, disclosure, alteration, or destruction. It involves implementing security controls, encryption mechanisms, access controls, and authentication measures to safeguard sensitive information and mitigate security risks.

- **Data integration and interoperability:** It refers to the ability of different systems, applications, and departments to share and use data effectively, despite differences in their data formats, structures, and protocols. This enables seamless communication, efficient data exchange, and informed decision-making across various domains in the public service.
- **Document and content management:** It focuses on organizing, storing, and retrieving data, such as documents, images, and multimedia files, to facilitate information sharing and collaboration within the department. It involves implementing document management systems, version control mechanisms, and search capabilities to manage the content lifecycle and ensure content integrity and accessibility.
- **Data warehousing and business intelligence management**: It involves designing, implementing, and managing data repositories and analytical tools to support decision-making and business intelligence initiatives. It encompasses data modelling, extraction, transformation, loading, reporting, and analytics capabilities to enable effective data-driven insights and decision-making.
- **Metadata management:** It involves managing metadata, which provides background information about data assets, such as data definitions, relationships, and lineage. It encompasses capturing, cataloguing, and governing metadata to facilitate data discovery, understanding, and lineage tracking across departmental systems and processes.
- **Data Quality:** It refers to the extent to which data is accurate, complete, consistent, reliable, and relevant for its intended use. It is a critical aspect of data management, as high-quality data is essential for informed decision-making, and effective departmental operations.

- **Reference and master data management**: It focuses on managing core data entities, such as customer, product, and employee information, to ensure consistency, accuracy, and integrity across department systems and applications. It involves defining data standards, establishing data ownership, and implementing processes for data synchronization and reconciliation. (DAMA, 2017)

Despite government having developed a legislative framework with implications for data management (**as outlined in section 5**), the public service remains without a coherent data management programme to support the implementation of such a legislative framework. **This framework seeks to institutionalize data governance in the public service as the key management practice of the data management programme.**

3. SCOPE

This framework is applicable to the public service as defined in section 195 of the Constitution as amended, namely:

- National departments.
- Provincial departments.
- National government components; and
- Provincial government component.

Furthermore, the framework applies to all data sets that are generated (including collection) by and or on behalf of departments as they deliver services to or transact with the citizens as well as part of the internal operations.

4. LEGISLATIVE MANDATE

While section 3(1)(f) of the Public Service Act of 1994, as amended, provides for the MPSA to establish norms and standards on information management for the public service, it is important to emphasize that there exists a legislative framework to regulate management of information (*inclusive of standards and regulations*) in the country. Below is the summary of the framework:

Legislation	Applicability
Constitution of the Republic of South Africa, 1996	Section 14(d) provides that Everyone has the right to privacy, which includes the right not to have the privacy of their communications infringed
Public Service Act 103 of 1994 (PSA)	Section 3 (1) (i) The Minister for the Public Service and Administration is responsible for establishing norms and

	standards for Information Management.
The Minimum Information Security Standards (MISS)	The Minimum Information Security Standards (MISS) is a government policy document that outlines the minimum-security measures institutions must take to protect sensitive and classified information. The purpose of the MISS is to protect national interests by ensuring that all institutions that handle sensitive or classified information maintain the standards.
Minimum Interoperability Standards (MIOS)	The Minimum Information Interoperability Standards (MIOS) sets out the Government's policies and standards for achieving interoperability and seamless information flow across government as well as the wider public sector.
Protection of Personal Information Act 4 of 2013 (POPIA)	POPIA introduces certain conditions so as to establish minimum requirements for the processing of personal information
Electronic Communications and Transactions Act 25 of 2002 (ECTA)	Chapter IX of the ECTA provides for the protection of critical databases including identification of critical data and databases; registration of critical databases; management of critical databases; restriction of disclosure of information; rights of inspection; and administration of none compliance.
Promotion of Access to Information Act 2 of 2000 (PAIA)	The object of the PAIA is to give effect to the constitutional right of access to any information held by the State and any information that is held by another required for the exercise or protection of any rights; and to provide for matters connected therewith.

Table 1: Legislative Framework

As indicated earlier, the above legislative framework has not translated into an established and well-coordinated data management programme in the public service despite the centrality of data in the current digital era. While this data governance framework seeks to facilitate the establishment of such a programme, its implementation will give effect to the envisioned outcomes of the above-mentioned legislative framework.

5. OBJECTIVE

The primary objective for this Data Governance Framework is to establish roles, responsibilities, structures, policies, practices, standards and process in relation to the management of data in the public service

6. OUTCOMES

The expected outcomes out of the implementation of this Data Governance Framework can be summarized as follows:

- Established roles, responsibilities, structures, practices, policies and processes in the management of data in the public service (**data stewardship**).
- Defined and enforced policies, practices, procedures, and standards for the management, protection, and utilization of data assets in the public service.
- Ensured compliance with relevant laws, regulations, and agreements governing the use of data assets.
- Established culture of data-driven decision-making, collaboration, and innovation in the public service.
- Enhanced quality, security, and value of data assets in the public service.
- An established data management programme in the public service prioritizing Data Governance practices.

7. GUIDING PRINCIPLES FOR DATA GOVERNANCE IN THE PUBLIC SERVICE

This framework shall be guided by a set of core principles that underpin the effective management of data across the public service. These principles are:

- **Leadership and strategy**: Data Governance should be guided by visionary and committed leadership as well as a data strategy that is informed by the departmental strategic plan.
- **Business driven**: Data Governance is a business-driven programme which should guide data related ICT initiatives as well as business interaction with data.
- **Shared responsibility**: Data Governance is the responsibility of all employees in the department.
- **Multi-layered:** Data Governance occurs at all levels of the department.

- **Framework based**: activities of the Data Governance programme must be based on an approved framework for effective coordination.
- **Principles based**: to ensure consistent application, the policy and activities emanating from the Data Governance programme must be based on a core set of principles.

8. BUSINESS DRIVERS FOR DATA GOVERNANCE IN THE PUBLIC SERVICE

As can be seen in section 5 of this framework, the South African government has established a robust legislative framework that requires largely public institutions (***including departments***) to establish specific practices regarding their management of data and or information assets. In line with this, the DPSA then conducted a data management maturity assessment (DMMA) during the 2021/22 financial year and the following issues were highlighted regarding data management by the departments:

- Data managed in silos within and between departments.
- Lack of common data definitions even for common data sets.
- Inadequate data quality management practices within and between departments leading to poor decisions.
- Unreliable data sources.
- Inadequate mechanisms to promote data sharing within and between departments.
- Duplicate data sets and information across the public service.

While the above-identified issues provide impetus to the data management programme in the public service, below are some of the common drivers for a data management programme across various sectors and organizations:

- The need to provide the necessary oversight and manage risks associated with the need for regulatory compliance with regards to data and information ***(personal, financial, etc.).***
- The need to treat and or manage data as a strategic asset upon which decisions, policies and interventions are based.
- The need to protect data assets through ensuring data availability, usability, integrity, consistency, auditability and security controls.
- The need to be able to respond efficiently, effectively and consistently to regulatory requirements.

- The need to continuously improve data quality thus positively impacting on business performance through reliable data.
- The need to manage metadata through defining and locating data in the organization.
- The need for data sharing between organizations (including internal sharing)
- The need to establish and ensure customer intimacy.\
- The need to introduce product/ service innovation.
- The need to ensure operational excellence.
- The need to control contracts dealing with data, e.g. purchase of data from third parties, cloud storage, sale of data as a product, etc.

The specific issues identified during the DMMA process in 2021 combined with the common drivers of data management mentioned above are important for organizations of all types. Consequently, it is specifically important for the public service to develop the required competencies, capabilities and practices to realize the intended outcomes associated with the country's legislative framework on data and information management. Lastly, organizations (including departments) that have reliable, high-quality data about their customers (the Citizens/ residents and organization), products, services and operations tend to make better and informed decisions than those that do not.

9. PROPOSED DATA GOVERNANCE STRUCTURES, ROLES AND RESPONSIBILITIES

Given that Executive Management is both accountable and often responsible for managing all aspects of the department, such must also include the management of data and information. Below are the minimum requirements to ensure that executive management provide the required leadership in ensuring that the department is aware of and protects data assets, allocate sufficient resources to optimize its usage and ensure that data risks are adequately managed across the public service.

9.1 Data Governance Committee

The Head of Department (HOD) must establish a Data Governance Committee (DGC) in the department which shall be a department wide cross-functional team or committee that is more representative of the business side of the organization than just the IT function. The DGC shall be the highest authority for data governance in the department (***a sub-committee of EXCO***)

with responsibility for oversight, support and allocation of resources to data governance activities. The committee will further oversee issues and escalations with regards to data governance and shall be chaired by the Chief Data Officer or any EXCO member. Membership to the DGC shall be dominated by the Data Owners or any delegated employee (***preferably a Business Data Steward***) who must be a member of the Senior Management Service (SMS) in the department, an IT as well as the legal representatives.

The core mandate of the DGC is to facilitate the development, approval as well as implementation of the department's Data Strategy and policies. Consequently, the DGC shall:

- Recommend the departmental data management programme including the data management strategy and data strategy for approval.
- Review and recommend the department's data architecture, policies, principles, standards and metrics for approval.
- Monitor compliance with legislative and regulatory requirements with regards to management of data in the department.
- Provide oversight into consistent and transparent use of data and information.
- Provide oversight to relevant data management sub-committees or working groups.
- Create internal alignment and communicate the data management programme in the department.
- Provide oversight into the management and resolution of data governance related issues.

As indicated earlier, data stewardship is central to effective data governance within a department requiring assignment of clear roles and responsibilities to ensure accountability. Consequently, the Head of Department shall establish a Data Governance Office **(DGO)** for the department to act as the implementation office responsible for executing the departmental data management programme.

9.2 Data Governance Office

The DGO shall, **only as an interim measure**, be an existing office performing activities either to coordinate planning (**Strategic plan**/ **Annual Performance Plan**) and or data/ information management and or operations across the department and or any other suitable/ relevant office guided by practices in the department. The DGO shall be the data management organization for the department under the leadership of the Chief Data Officer (CDO) responsible for:

- Working with the CDO in all data management activities of the department.
- Managing data access requests within and between departments guided by the information and or deputy information officer.
- Coordinating internal data management awareness training and communication.
- Monitoring and reporting on the departmental data governance key performance indicators.
- Establish the function and capabilities to track and enforce regulatory compliance and conformance to the data strategy, architecture, policies, standards, principles, and procedures.
- Coordinating all data management initiatives ***(data management cycle activities)*** in the department.

Despite providing technology capability to manage data through its lifecycle, **the Office of the GITO/ CIO shall not** be the DGO of the department. However, the DGO shall perform and coordinate its work leveraging capacity as well as capabilities (including technology) that exist across the department. As indicated earlier, DGO activities must contribute to the implementation of the data management programme for the department.

9.3 Chief Data Officer

Effective management of data must always seek to enable the achievement of business goals and objectives. Consequently, business must take the lead in the proper management of data in the department. To ensure that the data management programme is business driven (**instead of IT-driven**) and challenges related to data management are fully addressed, **the Head of Department must appoint the Chief Data Officer (CDO).** Generally, the CDO will be an Executive or Senior Manager who will assist in fulfilling the department's data and or information requirements in support of both the operational as well as service delivery goals and objectives of the department. Consequently, **the CDO shall**:

- Develop the business aligned data strategy, data architecture and data management strategy for the department.
- Ensure the approval of the department's data strategy, data architecture and data management strategy.
- Develop data management policies, standards, practices and procedures for the department.

- Lead the Data Management Maturity Assessment in the department.
- Establish and monitor adherence to metrics for all data management functions in the department.
- Champion the data management programme including communicating its importance to all the department's stakeholders.
- Ensure effective governance, storage, operations and analytics of data in the department.
- Collaborate with stakeholders to leverage data thus drive value for the department.

The CDO shall work with various stakeholders in the department, and this shall include assisting efforts to institutionalize the data ownership model in the department.

10. CONCEPTUAL DATA OWNERSHIP MODEL

In line with the guiding principles highlighted in section 7 of this framework, the program areas in the department must have an active and important role towards both the governance and management of data. Below is the conceptual Data Ownership model which the Head of Department must institutionalize through **assigning or designating** the various roles in the department. Such assignment will go a long way in ensuring an effective data governance programme or journey in the department.

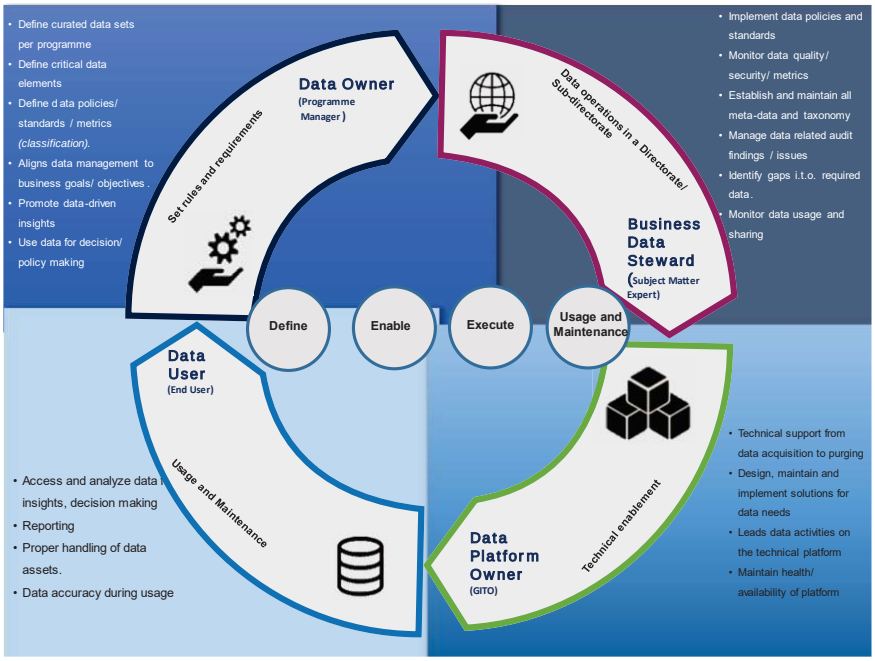


Figure 3: Conceptual Data Ownership Model

10.1 Data Owner

The Data Owner (DO) is one key role that must be designated in the department. The DO shall be a programme manager in the department whose responsibility is to ensure effective data management within his/ her programme (domain). Consequently, each department shall have more than one Data Owner, and s/he will be responsible for:

- Ensuring proper management of data related to a specific programme/ domain through setting data rules (**policies, processes and procedures**) and oversee their effectiveness.
- Defining and or confirming sub-programmes within the programme.
- Guiding, directing and managing the data stewards in the data management work to be done.
- Defining in-programme curated data sets as well as critical data elements.
- Reviewing and authorizing each data access request individually or defining a set of rules that determine who is eligible for access based on business function, support role, etc.
- Reviewing and approving data definitions, models and metadata for the programme.

- Performing activities to align and give effect to the CDO as well as the department's data management programme.

It is important to emphasize that the DO will work closely with various Business Data Stewards within the programme as well as other Data Owners in the department

10.2 Business Data Steward

The Business Data Steward shall be the subject matter expert in the programme area/ domain reporting to the Data Owner. The Data Owner shall be responsible for assigning or designating the Business Data Steward roles within the programme under his/ her responsibility while the Head of Department shall monitor that such action takes place. In essence, this role shall also be responsible for source ***(raw OR primary***) data at the stage when it is collected and or generated from various sources for processing at a later stage. In other words, the Business Data Steward deals with raw data that is not yet analysed and thus needs to be aware or conversant with the data origin, data format, data traceability to its source as well as the quantity and quality of data amongst other issues. In the context of a department, officials leading/ heading the sub-programmes as defined by the Data Owner may be better positioned to play this role given their proximity and or appreciation of the subject matter at hand. Consequently, the Business Data Steward shall:

- Identify and or define the credible source(s) of data to be collected and or generated in support of the programme.
- Identify and or determine categories of formats of collected and or generated data for processing at a later stage.
- Establish mechanisms for collected/ generated data to be traceable to its original source.
- Create and maintain all related meta-data and taxonomy within a progamme.
- Monitor that defined data security/ quality metrics are appropriately implemented.
- Manage data related audit findings within a programme through to closure.
- Identify gaps in the defined data requirements for programme success.
- Authorize data purging informed by business needs and regulatory requirements.

10.3 Data Platform Owner

Effective data management also depends on departments investing and using technologies with varied capabilities from data collection/ creation to storage, usage, maintenance and

disposal. by departments. Consequently, the Government Information Technology Officer (GITO) shall be assigned or designated the role of the data platform owner whose responsibility is to:

- Provide technical support from data acquisition to deletion/ archiving.
- Design, maintain and implement solutions to meet the department's data needs.
- Lead data focused activities on the technical platform.
- Implement the relevant and or defined data security levels in the platform.
- Monitor, report and resolve non-functional requirements ***(technology platform performance - managing platform health)***.
- Provide the disaster recovery capability and ensure the stability of the platform.

10.4 Data User

- The Data User is another key role player in the governance and management of data assets within a department. In essence, the Data User is also a subject matter expert within a specific programme area with the authority to use and or manipulate data of any programme or subject area for insights, decision making as well as policy making. Consequently, the Data User shall:
  - Access and analyze data for insights, decision making and policy development.
  - Generate subject matter specific reports informed by the analyzed data
  - Act in compliance with the department's data governance policies, standards and procedures.
  - Observe the existence of metadata standards to facilitate data integration across the department.
  - Comply with security measures and access control to the department's data.
  - Ensures that the Directorate's or sub-Directorate's data quality standard complies with the department's data quality policy or standard.

11. IMPLEMENTATION OF THE DATA GOVERNANCE PROGRAMME IN THE PUBLIC SERVICE

To ensure that data governance remains sustainable while embedded in the department, it must be implemented, monitored and adjusted in a continuous basis as part organizational practices and operations. This implies the identification and implementation of deliverables, activities, practices, processes as well as monitoring mechanisms to ensure the achievement

of the desired outcomes. Consequently, **the Head of Department must** implement a data governance programme as a matter of priority to improve the management of data in the department. Given that the implementation of the programme will introduce changes to management of data in the department, the programme implementation must be executed simultaneously with the change management intervention as the foundation or vehicle for introducing the changes. At minimum, the change management intervention must ensure that all affected people are **A**ware, **D**esire, have **K**nowledge, and are **A**ble to implement change on a continuous basis which must be ensured through some **R**e-inforcement activities. Such would, amongst other things, prompt the department to treat data more as a strategic asset.

While numerous models and frameworks around change management **(ADKAR)**, programme management **(Prince2, PMBOK, etc)** as well as continuous improvement **(Deming Cycle – Plan, Do, Check, Act)** can be adopted and adapted towards the implementation of the data governance programme, below is COBIT implementation approach that combines elements of these models and or frameworks and hence can be adopted and adapted accordingly by departments:

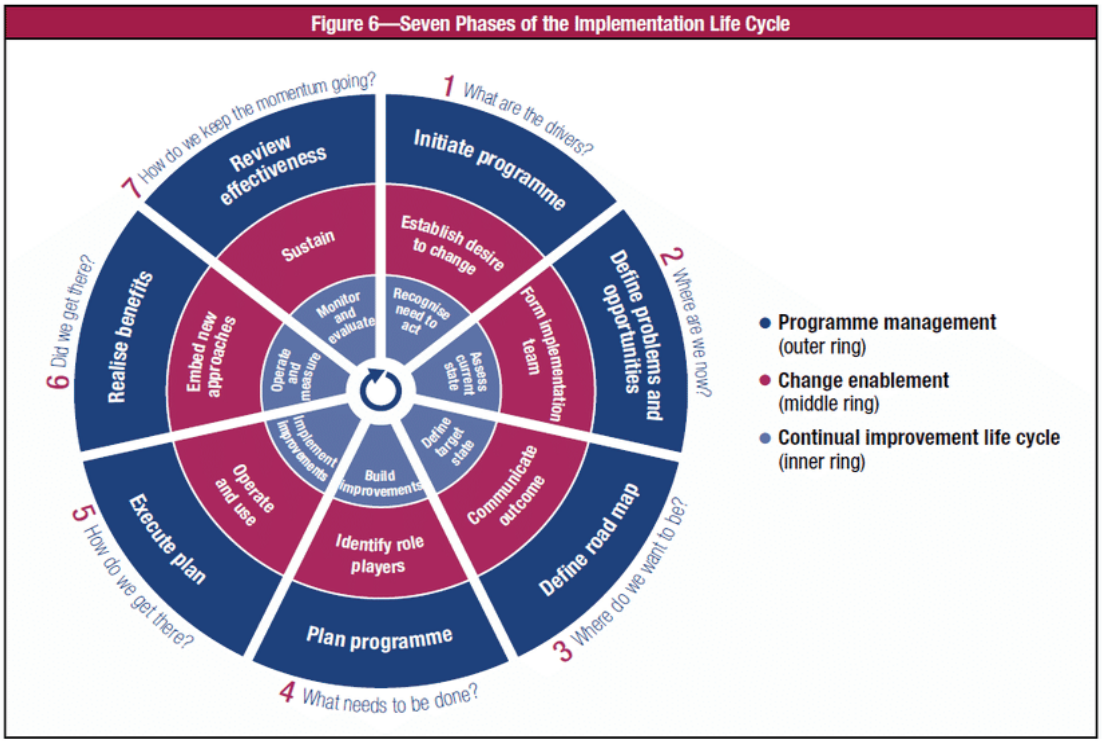


Figure 4: COBIT Implementation guide

Guided by the combination of above models and frameworks, the implementation of the data governance programme must be executed following the below mentioned phases.

1. **Establish the desire to change**

   During this phase, the department must establish "the desire to change" with regards to its data management capability and launch the programme. The Executive Management must take the lead and responsibility for initiating the programme guided by the departmental goals, objectives, challenges as well as opportunities facing the organization with regards to management of data. For departments, the need to comply with regulations (i.e PAIA, POPIA, etc) combined with the necessity for evidence-based decision making as well as policy making are more than sufficient drivers for improved data management. Furthermore, the centrality of data as the "crude oil" for socioeconomic activities in this digital economy may act as one of the drivers as well.

2. **Understand the current maturity level** *(As-Is)* **with regards to data management**

   During this phase, the department must establish or understand its existing data management maturity level. In the context of this framework, a department must conduct a data management maturity assessment (DMMA) as a starting point. For instance, the DMMA may highlight poor quality data, lack of credible data sources, data managed in silos and inadequate data security practices amongst other issues. The outcomes of DMMA will then highlight areas of weakness and strength in the department with regards to data management giving the opportunity for the identification of priority areas of intervention going forward. With this framework focusing on data governance, the state or maturity of policies, standards, practices, process, roles and responsibilities with regards to management of data must be outlined. The Capability Management Model Integration (CMMI) as outlined below can be used to assess the maturity level of the various data management knowledge areas.

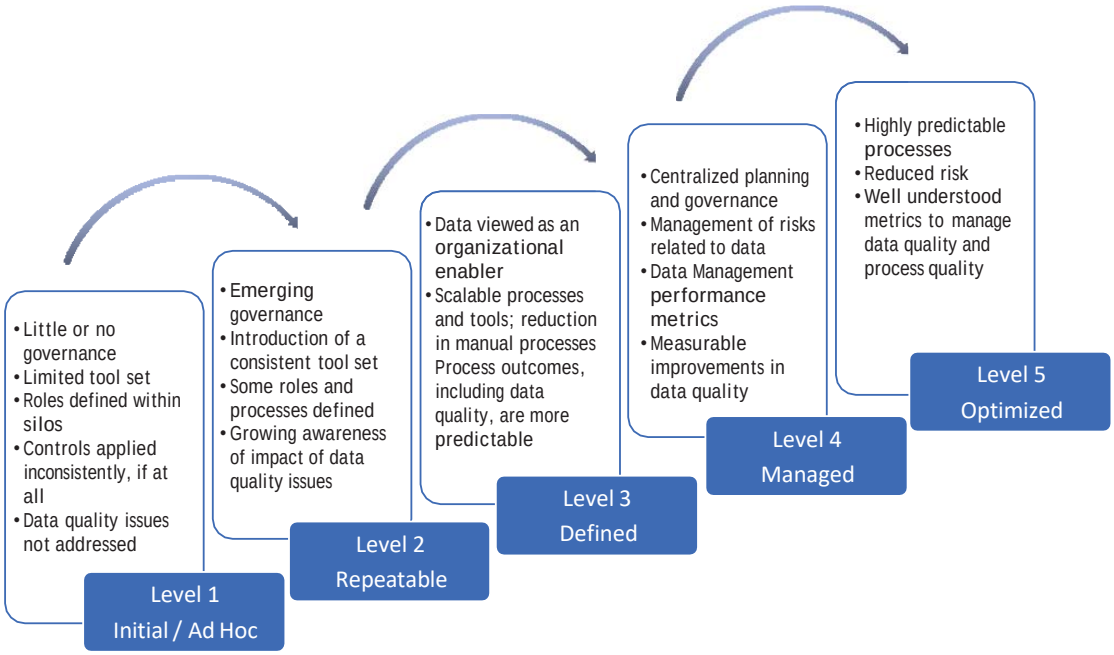


Figure 5: Data Management Maturity model *(Adapted from CMMI)*

Below is a summary of the data management maturity levels based on the CMMI:

Level 0: No Capability: An organization at this level has no organized data management practices or formal enterprise processes for managing data. Very few organizations exist at Level 0. This level is acknowledged as part of the maturity model for purposes of definition only.

Level 1 Initial / Ad Hoc: General-purpose data management using a limited tool set, with little or no governance. Data handling is highly reliant on a few experts. Roles and responsibilities are defined within silos. Each data owner receives, generates, and sends data autonomously. Controls, if they exist, are applied inconsistently. Solutions for managing data are limited. Data quality issues are pervasive but not addressed. Infrastructure support is at the business unit level.

Level 2 Repeatable: Emergence of consistent tools and role definition to support process execution. In Level 2, the organization begins to use centralized tools and to provide more oversight for data management. Roles are defined and

processes are not dependent solely on specific experts. There is organizational awareness of data quality issues and concepts. Concepts of Master and Reference Data begin to be recognized.

Level 3 Defined: Emerging data management capability. Level 3 sees the introduction and institutionalization of scalable data management processes and a view of DM as an organizational enabler. Characteristics include the replication of data across an organization with some controls in place and a general increase in overall data quality, along with coordinated policy definition and management. More formal process definition leads to a significant reduction in manual intervention. This, along with a centralized design process, means that process outcomes are more predictable.

Level 4: Managed: Institutional knowledge gained from growth in Levels 1-3 enables the organization to predict results when approaching new projects and tasks and to begin to manage risks related to data. Data management includes performance metrics. Characteristics of Level 4 include standardized tools for data management from desktop to infrastructure, coupled with a well-formed centralized planning and governance function. Expressions of this level are a measurable increase in data quality and organization-wide capabilities such as end-to-end data audits.

Level 5: Optimized: When data management practices are optimized, they are highly predictable, due to process automation and technology change management. Organizations at this level of maturity focus on continuous improvement. At Level 5, tools enable a view data across processes. The proliferation of data is controlled to prevent needless duplication. Well-understood metrics are used to manage and measure data quality and processes.

3. **Establish consensus on the desired** *(future state)* **data management maturity level**

During this phase, the department must establish or reach consensus on the desired

(future state) data management maturity level emanating from or informed by the DMMA outcomes. Related key performance indicators over a specific period must also be defined.

4. **Develop the roadmap** *(including the implementation plan)* **for the data management programme**

   During this phase, the department must develop the roadmap (including the implementation plan) for the data management programme. Given that data governance has been identified as a priority knowledge or focus area for improved data management, **projects to improve data governance** activities must also be identified first for implementation. For instance, the appointment and or designation of employees into specific data management roles, development of priority data standards and procedures, and other data governance activities must be prioritized towards the improvement of data management in the department. The key performance indicators for each knowledge or focus area of data management as well as the monitoring systems, mechanisms, must also be identified. Lastly, a programme plan highlighting the activities, deliverables and responsibilities must also be developed.

5. **Post Implementation Review**

   During this phase, the department must assess progress made (**or lack thereof**) towards the implementation of the data management programme. The outputs, outcomes and impact of implementing the programme must be assesses guided by, amongst other things, the KPIs identified during the roadmap development phase. The outputs, outcomes and impact must also be measured over a short **(0-12 months)**, medium **(18 - 60 months)** and long-term periods (**beyond 60 months**), with monitoring and assessment process or steps continuously taking place in every phase of the programme. Lastly, corrective actions in instances where targets have been missed will largely take place during this phase.

6. **Programme sustainability actions**

During this phase, the department must be preoccupied with activities and actions to ensure that the data management programme remains sustainable. While sustainability will largely depend on the extent of the alignment and or integration of the programme to the existing activities of the department, a strong and continuous communication campaign focusing on successes of the programme must be implemented. Where failures have been identified, the intention must be to ensure that the underlying causes are addressed. Additional data governance and management interventions required to make the programme a success can also be identified for implementation.

12. CONCLUSION

Successful management of data requires a proactive approach to addressing stakeholders' needs for high quality data, while protecting the privacy of individuals. To accomplish this the departments are required to develop and implement a comprehensive data governance programme that will help them to improve their decision making and efficiency of operations through coordinated responses to common issues such as data access controls and staff training; standardizing data definitions and processes, a core requirement for interoperability, and implementing a holistic approach to mitigating data security risk.

While this framework provides **annexure A** as the proposed high level implementation roadmap for the programme, departments are encouraged to develop their own roadmaps/ plans informed by their internal context, issues and priorities. Going forward, departmental performance will be measured against the proposed roadmap in the event they have not developed their own.

APPROVED BY THE MINISTER FOR PUBLIC SERVICE AND ADMINISTRATION

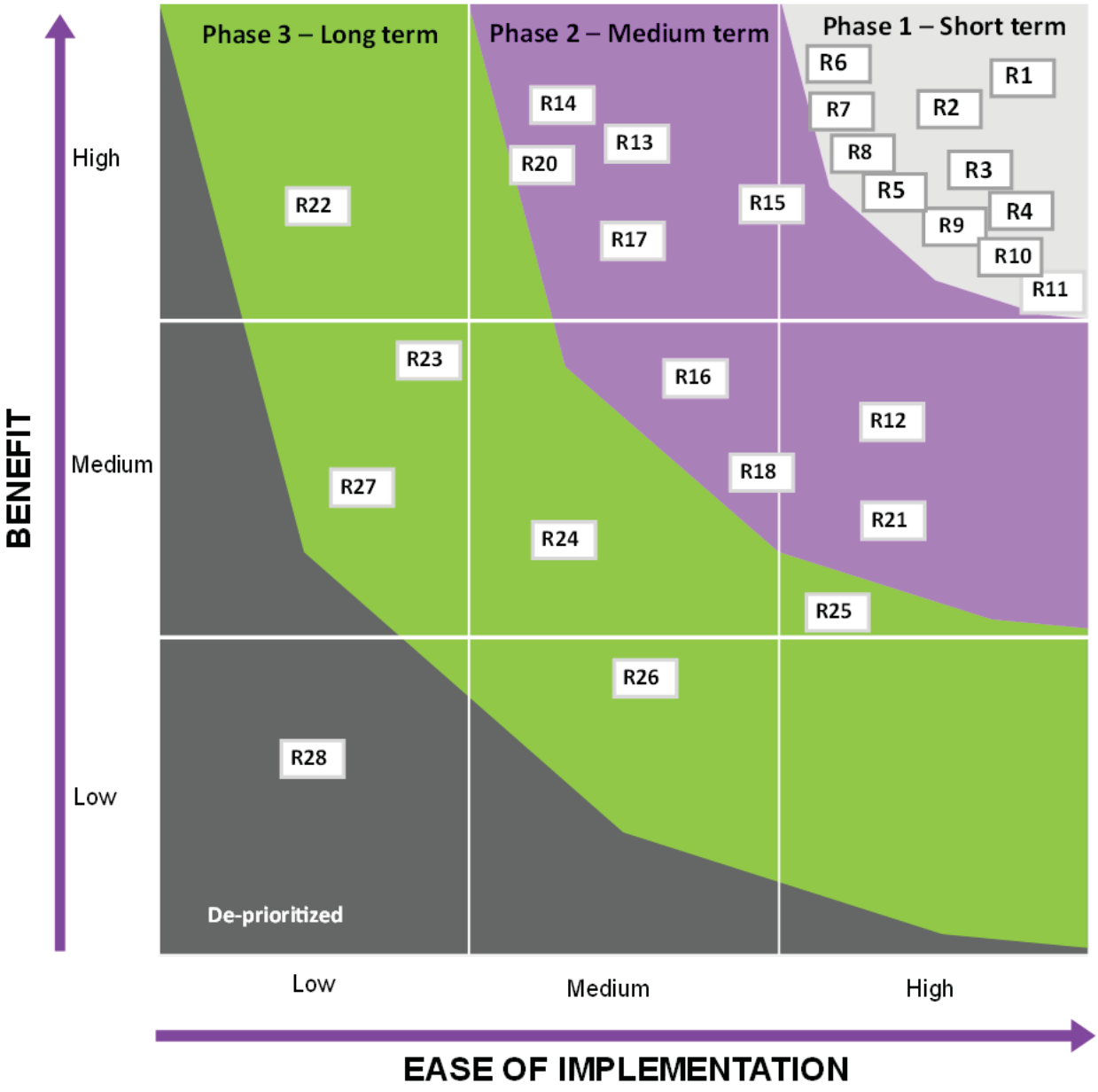
INKOSI MZAMO BUTHELEZI, MP

MINISTER FOR THE PUBLIC SERVICE AND ADMINISTRATION
DATE: 02/04/25

13. REFERENCES

1. COBIT 2019 Framework: Introduction and Methodology. 2018. ISACA, USA
2. COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution. 2018. ISACA, USA
3. Data Management Association (DAMA). (2017). DAMA: DMBOK: Data Management Body of Knowledge. 2nd ed. New Jersey: Technics Publications
4. Department of Communications and Digital Technologies. (2020). Summary Report and Recommendations presented by Commission on the Fourth Industrial Revolution; and Diagnostic Report of the Presidential Commission on the Fourth Industrial Revolution. Retrieved from http://www.gpwonline.co.za/Gazettes/Pages/Published-National-Government-Gazettes.aspx [Accessed 12 February 2021]
5. Department of Public Service and Administration (2007). Minimum Interoperability Standards v4.1. http://www.dpsa.gov.za/dpsa2g/egov_documents.asp [Accessed 9 December 2020]
6. Department of Telecommunications and Postal Services (2007). The National Information Society and Development (ISAD) Plan. Retrieved from https://www.dtps.gov.za/index.php?option=com_phocadownload&view=category&id=98&Itemid=401# [Accessed 23 February 2021]
7. Fleckenstein, M., & Fellows, L. (2018). Modern Data Strategy. Springer International Publishing AG 2018.
8. Gauteng Provincial Government (2019). Gauteng Provincial Government Big Data Strategy. Version 14.2b. 31 January 2019
9. Information Regulator of South Africa (2000). Promotion of Access to Information Act, 2000 (Act No. 2 of 2000). https://www.justice.gov.za/inforeg/docs.html [Accessed 17 December 2020]
10. Information Regulator of South Africa (2013). Protection of Personal Information Act, 2013 (Act No. 4 of 2013). https://www.justice.gov.za/inforeg/docs.html [Accessed 17 December 2020]
11. Western Cape Government (2019). Province-Wide Data Governance: Strategic Framework for Province-Wide Data Governance in the Western Cape Government. Volume 1. 1 February 2019

APPENDIX A: HIGH LEVEL DATA MANAGEMENT ROADMAP



Priority	Recommendation
R1	A Data Governance framework should be developed to guide all data management functions.
R2	Data Strategy: This should be defined, communicated, and executed for good data management.
R3	Establish a data governance committee, with representation from IT, business and assurance functions
R4	Establish a Data Office for the Department tasked with the delivery of the data strategy and road map.
R5	Establish Data Stewardship.
R6	Data Policies: Setting and enforcing policies related to data and metadata management, access, usage, security, and quality. Data policies must be effectively communicated, monitored, enforced, and periodically re-evaluated. Regular training on data governance policies should be done.
R7	Development of an Information & Data architecture blueprint for the Department. The blueprint should meet the current and long-term data requirements of Department.
R8	Build and deploy a robust data warehouse system, adopting effective BI tools, providing necessary training to staff, and establishing clear data governance policies and procedures.
R9	Develop a Data Quality framework: which outlines the organization's standards, processes, and responsibilities for ensuring data quality.
R10	Invest in Data Quality management tool: invest in and deploy a data quality tool. Implementing a data quality tool can greatly assist in identifying and correcting errors or inconsistencies in data. These tools can automate many aspects of data quality management, such as data profiling, cleaning, matching, and monitoring, making the process more efficient and effective.
R11	Implement a Metadata management Tool: to help the Department automate the metadata collection process, maintain consistency across the organization, and make metadata easily accessible and usable.
R12	Produce initial Data Architecture artifacts, such as enterprise data model and enterprise- wide data flow.
R13	Implement a Master Data Management System
R14	Establish a Metadata Standard for metadata creation, usage, and management.
R15	Compliance: Ensuring the organization can meet data-related regulatory compliance requirements.
R16	The Department to enhance the data storage infrastructure, improving the data operations procedures, investing in better database management systems, enhancing SLAs, and providing relevant training to staff.
R17	The Department to establish and manage data modelling & design practices. This involves developing and implementing data models, providing training for staff, and potentially hiring or consulting with experts in data modelling & design.
R18	Invest in Data Integration Tools: invest in advanced data integration tools that automate the process of extracting, transforming, and loading data from various sources into a unified format

Priority	Recommendation
R1	A Data Governance framework should be developed to guide all data management functions.
R2	Data Strategy: This should be defined, communicated, and executed for good data management.
R3	Establish a data governance committee, with representation from IT, business and assurance functions
R4	Establish a Data Office for the Department tasked with the delivery of the data strategy and road map.
R5	Establish Data Stewardship.
R6	Data Policies: Setting and enforcing policies related to data and metadata management, access, usage, security, and quality. Data policies must be effectively communicated, monitored, enforced, and periodically re-evaluated. Regular training on data governance policies should be done.
R7	Development of an Information & Data architecture blueprint for the Department. The blueprint should meet the current and long-term data requirements of Department.
R8	Build and deploy a robust data warehouse system, adopting effective BI tools, providing necessary training to staff, and establishing clear data governance policies and procedures.
R9	Develop a Data Quality framework: which outlines the organization's standards, processes, and responsibilities for ensuring data quality.
R10	Invest in Data Quality management tool: invest in and deploy a data quality tool. Implementing a data quality tool can greatly assist in identifying and correcting errors or inconsistencies in data. These tools can automate many aspects of data quality management, such as data profiling, cleaning, matching, and monitoring, making the process more efficient and effective.
R11	Implement a Metadata management Tool: to help the Department automate the metadata collection process, maintain consistency across the organization, and make metadata easily accessible and usable.
R12	Produce initial Data Architecture artifacts, such as enterprise data model and enterprise- wide data flow.
R13	Implement a Master Data Management System
R14	Establish a Metadata Standard for metadata creation, usage, and management.
R15	Compliance: Ensuring the organization can meet data-related regulatory compliance requirements.
R16	The Department to enhance the data storage infrastructure, improving the data operations procedures, investing in better database management systems, enhancing SLAs, and providing relevant training to staff.
	and platform. These tools often come with features to handle discrepancies in data structures and formats, making the integration process more efficient and less prone to errors.
R19	Development of Document and Content Management Standard.
R20	Provide Training and Build a Data-Centric Culture: Staff training is essential for the effective implementation of any data management practices. Training should be provided to staff on the

Priority	Recommendation
R1	A Data Governance framework should be developed to guide all data management functions.
R2	Data Strategy: This should be defined, communicated, and executed for good data management.
R3	Establish a data governance committee, with representation from IT, business and assurance functions
R4	Establish a Data Office for the Department tasked with the delivery of the data strategy and road map.
R5	Establish Data Stewardship.
R6	Data Policies: Setting and enforcing policies related to data and metadata management, access, usage, security, and quality. Data policies must be effectively communicated, monitored, enforced, and periodically re-evaluated. Regular training on data governance policies should be done.
R7	Development of an Information & Data architecture blueprint for the Department. The blueprint should meet the current and long-term data requirements of Department.
R8	Build and deploy a robust data warehouse system, adopting effective BI tools, providing necessary training to staff, and establishing clear data governance policies and procedures.
R9	Develop a Data Quality framework: which outlines the organization's standards, processes, and responsibilities for ensuring data quality.
R10	Invest in Data Quality management tool: invest in and deploy a data quality tool. Implementing a data quality tool can greatly assist in identifying and correcting errors or inconsistencies in data. These tools can automate many aspects of data quality management, such as data profiling, cleaning, matching, and monitoring, making the process more efficient and effective.
R11	Implement a Metadata management Tool: to help the Department automate the metadata collection process, maintain consistency across the organization, and make metadata easily accessible and usable.
R12	Produce initial Data Architecture artifacts, such as enterprise data model and enterprise- wide data flow.
R13	Implement a Master Data Management System
R14	Establish a Metadata Standard for metadata creation, usage, and management.
R15	Compliance: Ensuring the organization can meet data-related regulatory compliance requirements.
R16	The Department to enhance the data storage infrastructure, improving the data operations procedures, investing in better database management systems, enhancing SLAs, and providing relevant training to staff.
	importance of reference and master data, the standards and procedures for managing this data, and how to use the MDM system.
R21	Development of standards and procedures should be developed for managing reference and master data.

Priority	Recommendation
R1	A Data Governance framework should be developed to guide all data management functions.
R2	Data Strategy: This should be defined, communicated, and executed for good data management.
R3	Establish a data governance committee, with representation from IT, business and assurance functions
R4	Establish a Data Office for the Department tasked with the delivery of the data strategy and road map.
R5	Establish Data Stewardship.
R6	Data Policies: Setting and enforcing policies related to data and metadata management, access, usage, security, and quality. Data policies must be effectively communicated, monitored, enforced, and periodically re-evaluated. Regular training on data governance policies should be done.
R7	Development of an Information & Data architecture blueprint for the Department. The blueprint should meet the current and long-term data requirements of Department.
R8	Build and deploy a robust data warehouse system, adopting effective BI tools, providing necessary training to staff, and establishing clear data governance policies and procedures.
R9	Develop a Data Quality framework: which outlines the organization's standards, processes, and responsibilities for ensuring data quality.
R10	Invest in Data Quality management tool: invest in and deploy a data quality tool. Implementing a data quality tool can greatly assist in identifying and correcting errors or inconsistencies in data. These tools can automate many aspects of data quality management, such as data profiling, cleaning, matching, and monitoring, making the process more efficient and effective.
R11	Implement a Metadata management Tool: to help the Department automate the metadata collection process, maintain consistency across the organization, and make metadata easily accessible and usable.
R12	Produce initial Data Architecture artifacts, such as enterprise data model and enterprise- wide data flow.
R13	Implement a Master Data Management System
R14	Establish a Metadata Standard for metadata creation, usage, and management.
R15	Compliance: Ensuring the organization can meet data-related regulatory compliance requirements.
R16	The Department to enhance the data storage infrastructure, improving the data operations procedures, investing in better database management systems, enhancing SLAs, and providing relevant training to staff.
R22	Security Awareness and Training: There needs to be continual training and awareness programs in place to ensure that all employees understand their roles and responsibilities in maintaining data security. The training should be mandatory and a prerequisite for employee performance evaluation.

Priority	Recommendation
R1	A Data Governance framework should be developed to guide all data management functions.
R2	Data Strategy: This should be defined, communicated, and executed for good data management.
R3	Establish a data governance committee, with representation from IT, business and assurance functions
R4	Establish a Data Office for the Department tasked with the delivery of the data strategy and road map.
R5	Establish Data Stewardship.
R6	Data Policies: Setting and enforcing policies related to data and metadata management, access, usage, security, and quality. Data policies must be effectively communicated, monitored, enforced, and periodically re-evaluated. Regular training on data governance policies should be done.
R7	Development of an Information & Data architecture blueprint for the Department. The blueprint should meet the current and long-term data requirements of Department.
R8	Build and deploy a robust data warehouse system, adopting effective BI tools, providing necessary training to staff, and establishing clear data governance policies and procedures.
R9	Develop a Data Quality framework: which outlines the organization's standards, processes, and responsibilities for ensuring data quality.
R10	Invest in Data Quality management tool: invest in and deploy a data quality tool. Implementing a data quality tool can greatly assist in identifying and correcting errors or inconsistencies in data. These tools can automate many aspects of data quality management, such as data profiling, cleaning, matching, and monitoring, making the process more efficient and effective.
R11	Implement a Metadata management Tool: to help the Department automate the metadata collection process, maintain consistency across the organization, and make metadata easily accessible and usable.
R12	Produce initial Data Architecture artifacts, such as enterprise data model and enterprise- wide data flow.
R13	Implement a Master Data Management System
R14	Establish a Metadata Standard for metadata creation, usage, and management.
R15	Compliance: Ensuring the organization can meet data-related regulatory compliance requirements.
R16	The Department to enhance the data storage infrastructure, improving the data operations procedures, investing in better database management systems, enhancing SLAs, and providing relevant training to staff.
R23	Training staff on these tools and on the importance of data integration can enhance the organization's capacity to manage and utilize its data more effectively.
R24	Adopt Data Interoperability Standards: To enhance interoperability, the Department should adopt widely accepted data standards and protocols that enable seamless data exchange across different systems. This involves defining common data formats, terminologies, and APIs that

Priority	Recommendation
R1	A Data Governance framework should be developed to guide all data management functions.
R2	Data Strategy: This should be defined, communicated, and executed for good data management.
R3	Establish a data governance committee, with representation from IT, business and assurance functions
R4	Establish a Data Office for the Department tasked with the delivery of the data strategy and road map.
R5	Establish Data Stewardship.
R6	Data Policies: Setting and enforcing policies related to data and metadata management, access, usage, security, and quality. Data policies must be effectively communicated, monitored, enforced, and periodically re-evaluated. Regular training on data governance policies should be done.
R7	Development of an Information & Data architecture blueprint for the Department. The blueprint should meet the current and long-term data requirements of Department.
R8	Build and deploy a robust data warehouse system, adopting effective BI tools, providing necessary training to staff, and establishing clear data governance policies and procedures.
R9	Develop a Data Quality framework: which outlines the organization's standards, processes, and responsibilities for ensuring data quality.
R10	Invest in Data Quality management tool: invest in and deploy a data quality tool. Implementing a data quality tool can greatly assist in identifying and correcting errors or inconsistencies in data. These tools can automate many aspects of data quality management, such as data profiling, cleaning, matching, and monitoring, making the process more efficient and effective.
R11	Implement a Metadata management Tool: to help the Department automate the metadata collection process, maintain consistency across the organization, and make metadata easily accessible and usable.
R12	Produce initial Data Architecture artifacts, such as enterprise data model and enterprise- wide data flow.
R13	Implement a Master Data Management System
R14	Establish a Metadata Standard for metadata creation, usage, and management.
R15	Compliance: Ensuring the organization can meet data-related regulatory compliance requirements.
R16	The Department to enhance the data storage infrastructure, improving the data operations procedures, investing in better database management systems, enhancing SLAs, and providing relevant training to staff.
	ensure data from one system can be accurately interpreted and used by another. The standards adopted should align with the nature of the data and the specific requirements of the Department.
R25	Ongoing communications: Supporting a continual employee security-training program informing employees of safe computing practices and current threats. An ongoing program communicates that safe computing is important enough for management to support it.

Priority	Recommendation
R1	A Data Governance framework should be developed to guide all data management functions.
R2	Data Strategy: This should be defined, communicated, and executed for good data management.
R3	Establish a data governance committee, with representation from IT, business and assurance functions
R4	Establish a Data Office for the Department tasked with the delivery of the data strategy and road map.
R5	Establish Data Stewardship.
R6	Data Policies: Setting and enforcing policies related to data and metadata management, access, usage, security, and quality. Data policies must be effectively communicated, monitored, enforced, and periodically re-evaluated. Regular training on data governance policies should be done.
R7	Development of an Information & Data architecture blueprint for the Department. The blueprint should meet the current and long-term data requirements of Department.
R8	Build and deploy a robust data warehouse system, adopting effective BI tools, providing necessary training to staff, and establishing clear data governance policies and procedures.
R9	Develop a Data Quality framework: which outlines the organization's standards, processes, and responsibilities for ensuring data quality.
R10	Invest in Data Quality management tool: invest in and deploy a data quality tool. Implementing a data quality tool can greatly assist in identifying and correcting errors or inconsistencies in data. These tools can automate many aspects of data quality management, such as data profiling, cleaning, matching, and monitoring, making the process more efficient and effective.
R11	Implement a Metadata management Tool: to help the Department automate the metadata collection process, maintain consistency across the organization, and make metadata easily accessible and usable.
R12	Produce initial Data Architecture artifacts, such as enterprise data model and enterprise- wide data flow.
R13	Implement a Master Data Management System
R14	Establish a Metadata Standard for metadata creation, usage, and management.
R15	Compliance: Ensuring the organization can meet data-related regulatory compliance requirements.
R16	The Department to enhance the data storage infrastructure, improving the data operations procedures, investing in better database management systems, enhancing SLAs, and providing relevant training to staff.
R26	Set security requirements for vendors: Include data security requirements in service level agreements and outsourcing contractual obligations. SLA agreements must include all data protection actions.
R27	Regular Audits and Penetration Testing: The Department needs continual checks to ascertain to identify potential vulnerabilities and to ensure that all security measures are working as intended.

Priority	Recommendation
R1	A Data Governance framework should be developed to guide all data management functions.
R2	Data Strategy: This should be defined, communicated, and executed for good data management.
R3	Establish a data governance committee, with representation from IT, business and assurance functions
R4	Establish a Data Office for the Department tasked with the delivery of the data strategy and road map.
R5	Establish Data Stewardship.
R6	Data Policies: Setting and enforcing policies related to data and metadata management, access, usage, security, and quality. Data policies must be effectively communicated, monitored, enforced, and periodically re-evaluated. Regular training on data governance policies should be done.
R7	Development of an Information & Data architecture blueprint for the Department. The blueprint should meet the current and long-term data requirements of Department.
R8	Build and deploy a robust data warehouse system, adopting effective BI tools, providing necessary training to staff, and establishing clear data governance policies and procedures.
R9	Develop a Data Quality framework: which outlines the organization's standards, processes, and responsibilities for ensuring data quality.
R10	Invest in Data Quality management tool: invest in and deploy a data quality tool. Implementing a data quality tool can greatly assist in identifying and correcting errors or inconsistencies in data. These tools can automate many aspects of data quality management, such as data profiling, cleaning, matching, and monitoring, making the process more efficient and effective.
R11	Implement a Metadata management Tool: to help the Department automate the metadata collection process, maintain consistency across the organization, and make metadata easily accessible and usable.
R12	Produce initial Data Architecture artifacts, such as enterprise data model and enterprise- wide data flow.
R13	Implement a Master Data Management System
R14	Establish a Metadata Standard for metadata creation, usage, and management.
R15	Compliance: Ensuring the organization can meet data-related regulatory compliance requirements.
R16	The Department to enhance the data storage infrastructure, improving the data operations procedures, investing in better database management systems, enhancing SLAs, and providing relevant training to staff.
R28	Train and encourage a Metadata-Centric Culture.

APPENDIX B: DEPARTMENTS MUST POPULATE THE RACI CHART INFORMED BY CONTEXT

Task/ Activity	Head of Department	Chief Data Officer	Data Owners	Business Data Stewards	Platform Owner	Data User	Legal
Establish the Data Governance Committee							
Establish the Data Governance Office							
Define data strategy							
Approve data strategy							
Implement data strategy							
Define data management strategy							
Approve data management strategy							
Implement the data management strategy							
Define data policies and standards							
Approve data policies and standards							
Implement data strategy, policies and standards							
Monitor and enforce policy compliance							
Identify and address data quality issues							
Manage data security and privacy							
Establish and maintain metadata							
Develop and maintain data architecture							
Facilitate data integration							
Support business intelligence initiatives							
Report on data governance progress							