Republic
of Rwanda

NISR
NATIONAL INSTITUTE OF
STATISTICS OF RWANDA

National Data Governance Framework

Table of Contents

Chapter 1

Introduction

Rwanda's vision to become a smart nation and a regional innovation hub depends on the effective use of high-quality, accessible, and secure data. Well-governed data is a strategic asset that underpins evidence-informed policymaking, enhances service delivery, drives innovation, and accelerates national transformation.

In this context, data governance is not only a technical requirement but a national priority. A consistent and collaborative approach across ministries, departments, and affiliated agencies ensures that data is managed as a shared resource contributing to the well-being of citizens and to Rwanda's sustainable development.

The National Data Governance Framework provides a common foundation for realizing this ambition. It establishes principles, standards, and institutional mechanisms to maximize the value of government data, safeguard privacy and confidentiality, and align national practices with international norms. Through strong governance, Rwanda will advance data quality, enable interoperability, encourage trusted data sharing, and build a culture of openness and innovation.

As mandated by the Government of Rwanda through the National Data Sharing Policy, the National Institute of Statistics of Rwanda (NISR) leads the data governance effort through the development of principles and standards for data governance to ensure stewardship, coherence, and accountability across the data ecosystem. Each Government of Rwanda (GoR)[1] institution will adopt these standards, creating a decentralized and coordinated data governance model.

The Rwanda Information Society Authority (RISA) provides the technological backbone and digital infrastructure required to bring these standards to life. As the leader in systems, platforms, and interoperability frameworks, RISA ensures that the technical environment supports secure data exchange, modern digital services, and innovation.

Together, NISR and RISA provide the policy, standards, and technology leadership needed to embed effective data governance across government. This partnership positions data as a driver of national competitiveness, ensuring that data and metadata are discoverable, interoperable, and machine-readable, which will unlock opportunities for innovation, research, and inclusive growth.

For citizens, effective data governance will translate into tangible benefits. It will mean faster and more reliable access to services without repeated paperwork, stronger protection of personal information, and greater confidence in how their data is managed. By reducing duplication and enhancing service efficiency, citizens will experience a government that is more responsive, transparent, and accountable

1 Government of Rwanda (GoR) in this framework means all public institutions and government-affiliated entities in Rwanda, including ministries, departments, agencies, local governments, and state-owned enterprises.

1.1. Current Data Governance Challenges

While Rwanda has made significant progress in digital transformation and institutional coordination, several challenges continue to limit the full potential of government data:

- Fragmented data silos: GoR institutions often operate in isolation, limiting the ability to integrate and share information.
- Inconsistent data quality: Variations in metadata, classification, and documentation reduce reliability and comparability across institutions.
- Capacity gaps: Technical expertise in advanced data management, governance, and analytics remains uneven across public institutions.
- Limited interoperability: Many systems are not yet designed for seamless integration, creating duplication and inefficiencies.
- Emerging risks: Growing volumes of data, alongside the rise of AI and big data, introduce new risks related to privacy, ethics, and cybersecurity.

Recognizing these challenges underscores the importance of a unified National Data Governance Framework. Addressing them will ensure Rwanda builds a secure, interoperable, and citizen-centered data ecosystem that accelerates transformation while safeguarding public trust.

1.2. Vision of National Data Governance

The vision is to build a coordinated, trusted, and citizen-centered national data ecosystem where government institutions securely manage and share data using common standards and interoperable systems. This ecosystem will ensure that data is accurate, timely, and ethically used to improve public services, strengthen accountability, foster innovation, and drive inclusive socio-economic development

This vision will be realized through the implementation of common standards and the establishment of a national data infrastructure[2] enabling unique identifiers across domains, such as individuals, businesses, and locations, allowing seamless integration of data from different sectors. This foundation will break down institutional silos, establish seamless interoperability between systems, and strengthen the integration of administrative data as a primary source for producing reliable official statistics.

The framework aspires to:

- Promote trust and accountability in government data through transparent processes, ethical use, and robust protection of citizens' information.
- Enable the interoperability and integration of data from multiple systems across GoR entities through unique identifiers and common standards
- Strengthen the use of administrative data for timely, cost-effective, and high-quality official statistics to support national development priorities.
- Build national capabilities in data management, analytics, and innovation to support responsive and high-quality decision-making.

2 National Data Infrastructure is the backbone that connects key information, such as people, businesses, and locations, through unique identifiers, making data reliable, consistent, and usable across government and sectors.

- Enhance the value of public sector data as a strategic asset for governance, economic growth, and digital transformation.

With this vision, Rwanda seeks to establish itself as a regional leader in data governance by setting standards that ensure reliable, high-quality, and accessible data for policymaking, public engagement, and innovation. The framework draws on international best practices, including the OECD Data Governance Principles, the DAMA DMBoK guidelines, and the African Union Data Policy Framework, to promote innovation-driven, citizen-centered, and ethical data governance.

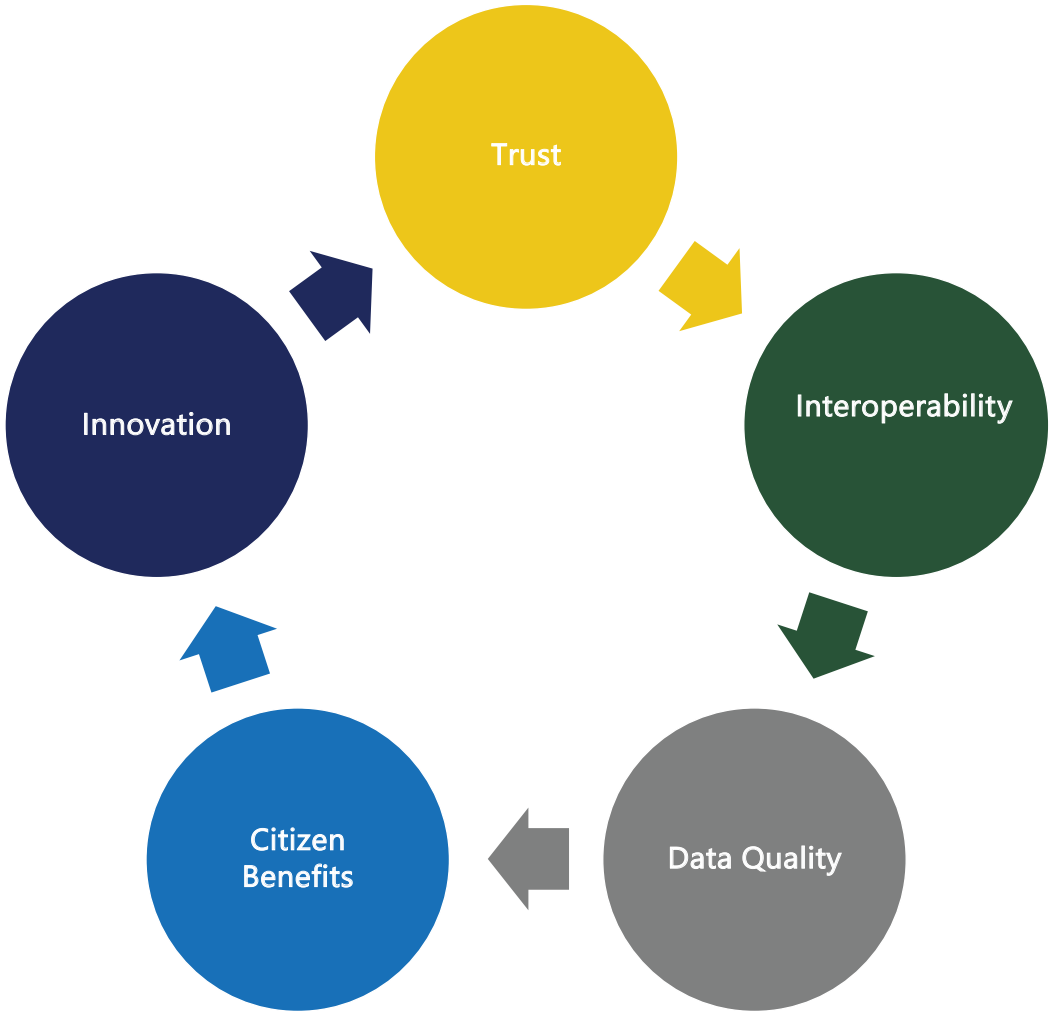

Figure 1: Rwanda's Data Governance Vision

1.3. Strategic Alignment with National Policies and Strategies

The National Data Governance Framework is closely aligned with Rwanda's broader national vision and strategic objectives, ensuring it supports the country's development, digital transformation, innovation, and evidence-based governance goals. It draws guidance from, and contributes to, the following key policies and strategies:

- **National Strategy for Transformation NST2:** Supporting economic transformation through data-driven innovation and public sector efficiency; advancing social transformation via evidence-based policy in health, education, agriculture, and social protection; and strengthening transformational governance through improved transparency and citizen participation.
- **Statistical Law No. 45/2013:** Ensuring compliance with legal frameworks governing official statistics; designating the National Institute of Statistics of Rwanda (NISR) as custodian of data governance and data stewards of the government of Rwanda.
- **Rwanda Data Protection and Privacy Law (Law No. 058/2021):** Ensuring responsible and lawful handling of personal data within government institutions.
- **National Data Revolution Policy (2017):** Operationalizing the use of big data, open data, and analytics for national development, reinforcing data accessibility, quality, interoperability, and reuse.
- **National Strategy for the Development of Statistics (NSDS4, 2024–2029):** Positioning administrative data as a key source for official statistics to improve timeliness and granularity of data; enhancing data quality, metadata management, and interoperability aligned with the National Data Infrastructure.
- **Rwanda National Artificial Intelligence Policy (2023):** Promoting responsible AI adoption grounded in high-quality, well-governed data, supported by ethical governance, privacy safeguards, and unique identifiers.
- **Digital Transformation Strategy for Rwanda (ICT Master Plan, 2021–2025):** Aligning with the national goal of a data-driven digital economy; supporting smart government services, e-governance, and the National Interoperability Framework.
- **SMART Rwanda Master Plan:** Leveraging ICT for improved service delivery and socio-economic growth through integrated government data systems and unique identifiers.
- **Rwanda Economy Digitalization Programme:** Facilitating transition to a fully digital economy with data as a critical economic asset; supporting establishment of a National Data Infrastructure for secure data exchange across government and private sectors.

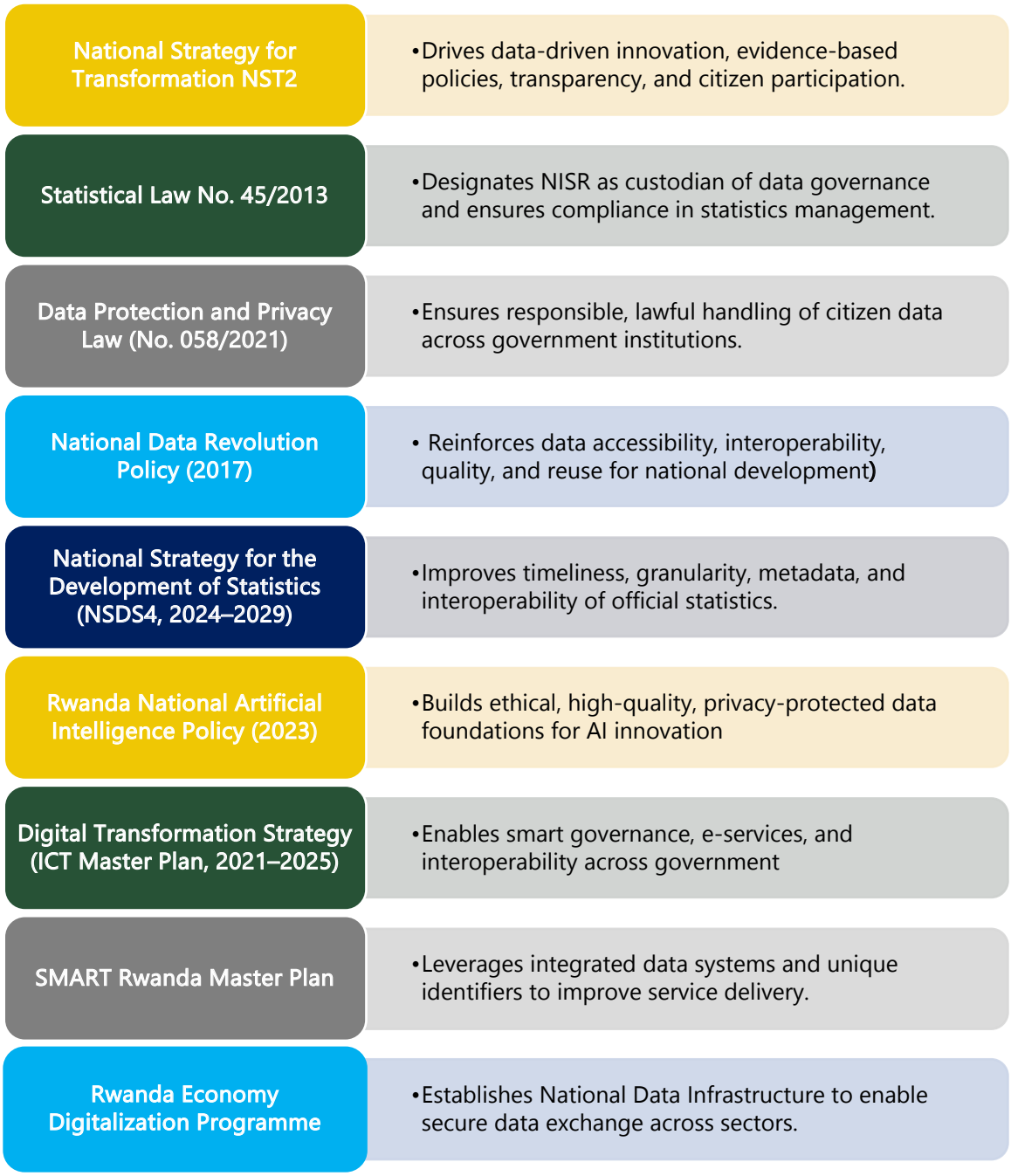

Figure 2 : Strategic Alignment with National Policies and Strategies

Through this strategic alignment, the Data Governance Framework enables Rwanda to realize its ambition of becoming a knowledge-based economy by 2050. It empowers government institutions to manage data as a strategic, well-governed asset, leveraging unique identifiers, administrative data integration, and ethical AI, to accelerate development, strengthen public trust, and drive innovation across all sectors.

Chapter 2

Purpose and scope of framework

2.1. Purpose

The purpose of this framework is to provide a unified, citizen-centered approach to managing government data as a national asset. It ensures accountability, quality, and security across the entire data lifecycle, from creation to secure disposal, and empowers institutions to use data responsibly for improved decision-making, service delivery, and innovation

The goal is to promote the adoption of a data governance framework based on internationally recognized standards that drive continuous improvement in data quality and value. The framework defines procedures, roles, and responsibilities for managing data throughout its entire lifecycle, from creation and collection to archiving and secure disposal.

To achieve these aims, all GoR institutions must:

- Implement an institutional model with clearly defined structures and roles to assign responsibility and accountability for data governance.
- Establish effective management and communication channels to coordinate data governance activities internally and across government entities.
- Enforce mandatory standards for data lifecycle management, metadata, and quality assurance.
- Maintain essential data governance artifacts, including definitions, visibility protocols, quality metrics, usage policies, and lineage documentation.
- Ensure full compliance with applicable national laws, regulations, and international standards on data management and protection.
- Guarantee that data shared with other government bodies is accurate, complete, timely, and protected according to its sensitivity and intended use.
- Protect government data from internal and external risks, including breaches of privacy, confidentiality, and cybersecurity.

By achieving these objectives, the framework will deliver measurable outcomes, including:

- Faster and more integrated service delivery through interoperable systems.
- Improved policy and planning supported by timely, reliable data.
- Stronger protection of citizen rights and privacy.
- Increased efficiency by reducing duplication of data collection and storage.
- Enhanced trust in government through transparent and ethical use of data.

2.2. Scope

The framework applies to all data and records managed by the Government of Rwanda, regardless of the format or location. This scope includes structured and unstructured data, digital and physical records, as well as metadata associated with these assets. It also applies to data exchanged in public-private partnerships, open data initiatives, and citizen-generated data when used for policy or service delivery purposes. It covers all personnel handling government data, including staff and contractors. While it sets high-level governance requirements, detailed policy development and implementation remain the responsibility of each institution. Private sector and non-governmental data not directly managed or mandated by the Government of Rwanda fall outside the scope of this framework, though alignment with its principles is strongly encouraged in collaborative initiatives.

Chapter 3

Data Governance Guiding Principles

The following guiding principles shall provide the foundation for the National Data Governance Framework. They shall guide all GoR institutions in managing data as a strategic national asset. They ensure that data is governed in a manner that promotes trust, accountability, innovation, and sustainable development.

Principle 1: Integrity

The Government of Rwanda shall ensure that all data is managed with integrity, honesty, and ethics. Data shall not be manipulated, misrepresented, or used in ways that undermine trust. All institutions and individuals handling data are required to act responsibly to safeguard data as a reliable foundation for evidence-informed decision-making.

Principle 2: Accountability and Stewardship:

The Government of Rwanda shall establish clear accountability for data at all levels. Data Owners[3] shall be formally designated and held responsible for decisions relating to the collection, use, sharing, and protection of data. Data Stewards [4]shall be appointed to ensure the consistent application of standards, maintain metadata, monitor quality, and oversee day-to-day data practices. Together, accountability and stewardship shall guarantee that data is managed effectively throughout its lifecycle.

Principle 3: Ethical and Citizen-centred Use:

The Government of Rwanda shall ensure that all data is collected, managed, and used in ways that respect the protection of personal data and privacy law, protect individual dignity, and promote fairness and inclusivity. Data shall not be exploited for purposes that undermine public trust, and governance practices shall prioritize citizens' interests, accessibility, and transparency.

Principle 4: Transparency:

The Government of Rwanda shall promote transparency in all data governance processes. Policies, standards, and procedures shall be documented and made accessible to stakeholders. Metadata and data lineage shall be maintained to provide clarity on the origin, transformation, and intended use of data, thereby ensuring confidence and trust in its quality and reliability.

Principle 5: Data Quality:

The Government of Rwanda shall ensure that data is accurate, complete, consistent, timely, and fit for purpose. All institutions shall implement robust data quality frameworks and adopt continuous monitoring, validation, and improvement practices to guarantee that data meets the requirements of decision-makers and users.

3 Data Owner is a senior leader or department head with ultimate authority over datasets; accountable for how data is used, protected, and aligned with business objectives.

4 Data Stewards are custodians responsible for maintaining data quality, consistency, and correct usage according to policies and standards.

Principle 6: Compliance

The Government of Rwanda shall require all data practices to comply with applicable laws, regulations, national policies, and international standards. Institutions shall implement mechanisms for monitoring and enforcement to ensure full adherence to legal and policy obligations, including the protection of data privacy, confidentiality, and intellectual property rights.

Principle 7: Security and Privacy

The Government of Rwanda shall safeguard all data against unauthorized access, misuse, or loss by adopting strong security measures. Personal and sensitive data shall be protected in line with legal and ethical requirements, ensuring the right to privacy is upheld. Institutions shall implement security and privacy controls that strengthen public confidence in the use of data.

Principle 8: Standardization and Interoperability

The Government of Rwanda shall promote the use of standardized definitions, classifications, formats, and coding systems across institutions. Standardization shall ensure consistency and comparability of data, while interoperability shall enable seamless data sharing and integration across government systems and with authorized partners. This shall eliminate duplication, enhance efficiency, and facilitate cross-sector collaboration.

Principle 9: Sustainability and Innovation

The Government of Rwanda shall embed continuous improvement and adaptability into data governance. Institutions shall anticipate and respond to emerging technologies such as AI, big data, and cloud services, ensuring that governance frameworks remain relevant, resilient, and innovation-friendly.

Principle 10: Value Creation

The Government of Rwanda shall govern data as a strategic national asset to maximize its value. Well-managed data shall be leveraged to drive innovation, improve service delivery, strengthen accountability, and

inform evidence-informed policymaking. Data governance shall ensure that the benefits of data are realized for economic growth and sustainable development.

Figure 3: Data Governance Guiding Principles

Chapter 4

Benefits of Data Governance for government institutions and citizens

Effective data governance provides numerous advantages for government institutions, including:

- **Improved data visibility and understanding:** It establishes data catalogues and glossaries that clarify data definitions, lineage, ownership, and stewardship, ensuring consistent use and unlocking greater data value.
- **Promotion of digital innovation and data literacy:** It facilitates access to meaningful data, encouraging self-service analytics, better performance measurement, and fostering innovation across government entities.
- **Enhanced data security, privacy, and compliance:** it ensures adherence to national and international data protection laws and standards, reducing risks of breaches and misuse of sensitive information.
- **High-quality data:** Data governance is a key building block in supporting data accuracy, completeness, consistency, and reliability, which is essential for effective governance and service delivery.
- **Strengthened integration and interoperability:** It defines clear data management processes that enable seamless data sharing within government and with external partners, supporting organizational agility.
- **Enhanced data analytics capabilities:** It provides trusted, well-curated data that supports advanced analytics, business intelligence, and AI projects, improving efficiency and impact.
- **Improved decision-making:** Empowers users with timely and reliable trusted data to make informed decisions that enhance service delivery and policy effectiveness.
- **Increased trust among stakeholders:** Builds confidence among government institutions by ensuring responsible, auditable data management.
- **Controlled broader data access:** It balances openness with protection through appropriate data classification and access controls, promoting discovery and transparency while safeguarding sensitive information.
- **Citizen-Centered Impact:** Beyond institutional advantages, strong data governance delivers direct benefits to citizens. It reduces duplication in service delivery, shortens turnaround times by reusing existing data (such as IDs and business registrations), and ensures personal information is safeguarded. Citizens experience greater trust and confidence in government services when data is managed transparently and ethically.

Collectively, these benefits reinforce Rwanda's broader national goals under the National Strategy for Transformation (NST2), the Smart Rwanda Master Plan, and the Digital Transformation Strategy. By institutionalizing data governance, government entities contribute not only to efficiency and innovation but also to the country's long-term vision of becoming a knowledge-based economy.

Chapter 5

Data Governance Operating Model

The Government of Rwanda will adopt a federated data governance operating model that combines central coordination with decentralized implementation. This ensures consistency across all public institutions while allowing flexibility to meet sector-specific needs.

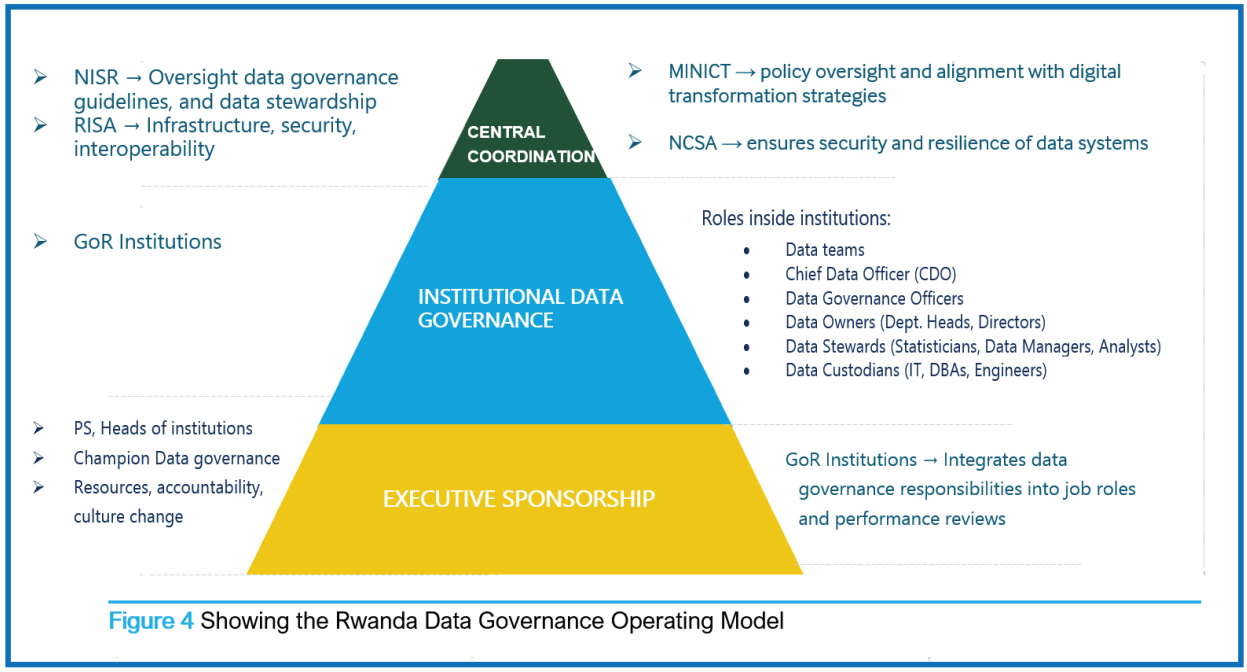

Figure 4 Showing the Rwanda Data Governance Operating Model

5.1. Central Coordination (National Level) and its responsibilities

The National Institute of Statistics of Rwanda (NISR) is designated as the official custodian of data governance [5]within the GoR. It holds the central responsibility for developing, maintaining, and enforcing national data governance frameworks, standards, and policies. This includes overseeing the quality, integrity, compliance, and proper use of government data, particularly statistical data, to ensure alignment with laws such as the Statistical Law (Law No. 45/2013) and the Data Protection and Privacy Law (Law No. 058/2021).

NISR's key roles include:

- Playing the role of data steward [6]for the Government of Rwanda
- Setting and regularly revising national data governance standards and guidelines.
- Providing strategic oversight and guidance to GoR on implementing data governance guidelines.

5 The National Data Sharing Policy provides NISR responsibility for providing oversight, technical guidance, and institutional support for data governance activities across the Government of Rwanda (GoR) entities, in line with national guidelines, standards, and applicable legal frameworks.

6 In this context, "data steward" NISR is legally mandated as a custodian of government data. While it is not the owner of all institutional datasets, it holds the responsibility to establish and enforce standards, safeguard data integrity and quality, promote interoperability, and oversee the responsible management and use of data across public institutions to support evidence-informed policymaking and national development.

- Leading capacity building, training, and awareness initiatives on data ownership, stewardship, and compliance.
- Monitoring and evaluating the effectiveness of data governance practices across government.
- Establishing compliance tools such as regular audits, performance scorecards, and certification mechanisms to ensure adherence across all institutions

To avoid duplication, NISR and RISA shall maintain a joint coordination mechanism that clarifies boundaries: NISR leads on policy, data quality, and compliance; RISA leads on infrastructure, interoperability, and cybersecurity. A joint annual coordination plan will be published to ensure alignment.

Rwanda Information Society Authority (RISA) complements NISR by managing the digital infrastructure and security aspects necessary for effective data governance. It is responsible for:

- Providing the technology needed to enable data governance
- Establishing and enforcing ICT standards, cybersecurity policies, and interoperability frameworks that safeguard government data.
- Providing technical support to secure data storage, transmission, and access controls.
- Enabling seamless and secure data sharing across government agencies and with external partners.

Collaborating with NISR to ensure the implementation of data governance guidelines.

5.2. Institutional Data Governance (Decentralized Level)

GoR institutions are accountable for implementing data governance guidelines aligned with the standards and guidance provided by NISR, as well as the ICT and security requirements set by RISA. Specifically, institutions must:

- Implement national data governance guidelines and adapt them to sector-specific needs.
- Appoint Data Owners, data governance officer [7], Data Stewards, and Data Custodians [8].
- Maintain data inventory, classification, and metadata in line with the standards set by NISR as the Central Coordinator.
- Comply with applicable laws and regulations regarding data management and protection.
- Establish internal governance structures with clearly defined roles and responsibilities to ensure accountability for data quality, security, and compliance.
- Collaborate actively with NISR and RISA by providing feedback, sharing performance data, and participating in capacity-building activities.

7 Data Governance Officer is a staff who coordinates policies, monitors compliance, and facilitates collaboration across data roles.

8 Data Custodian is an IT and technical staff responsible for implementing controls, storing, securing, and maintaining data infrastructure.

In addition to their internal responsibilities, institutions will participate in inter-ministerial Data Governance Working Groups convened by NISR and RISA. These groups will share lessons, resolve interoperability challenges, and harmonize practices across sectors.

5.3. xecutive Sponsorship: Leadership Commitment and Support

Effective data governance requires strong commitment from senior leadership within each GoR institution. They provide the leadership and resources necessary for sustained success.

In general Executive sponsors play a critical role in:

- Championing data governance initiatives and embedding them into institutional priorities and culture.
- Allocating necessary resources, including budget, personnel, and technology, to support governance activities.
- Empowering data owners, stewards, and governance teams to carry out their responsibilities effectively.
- Ensuring accountability by reviewing governance performance reports and enforcing corrective actions where needed.
- Facilitating cross-departmental collaboration and removing institutional barriers to data governance.
- Communicating the value and importance of data governance to all staff and stakeholders, fostering a data-driven mindset.

The operating model is ultimately designed not only to strengthen institutional efficiency but also to improve citizen outcomes, reducing duplication in service delivery, protecting privacy, and enabling faster, more reliable access to government services through interoperable systems.

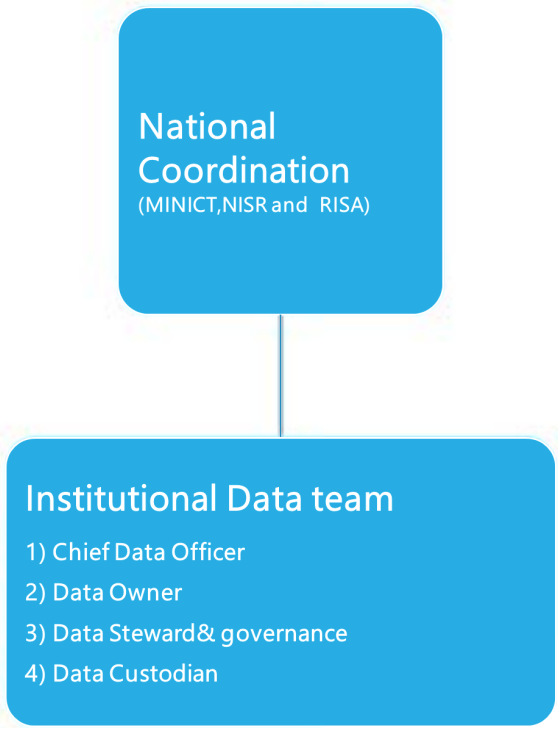

Figure 5 Federated Data Operating Model

Chapter 6

Establishing a program for data governance

For data governance to deliver real value, each government institution must establish a formally structured and well-supported program. This program should be proportionate to the institution's size, mandate, and available capabilities, ensuring that governance activities are both practical and sustainable. While the design may vary, certain core elements are non-negotiable to ensure the continuous and consistent practice of data governance across the Government of Rwanda (GoR).

To support practical implementation, institutions should adopt a phased roadmap that allows progressive maturity:

- **Phase 1:** Establish governance structures, assign roles, and develop baseline policies.
- **Phase 2:** Roll out data catalogues, classification, and quality management processes.
- **Phase 3:** Integrate governance into analytics, AI, and service delivery innovations.

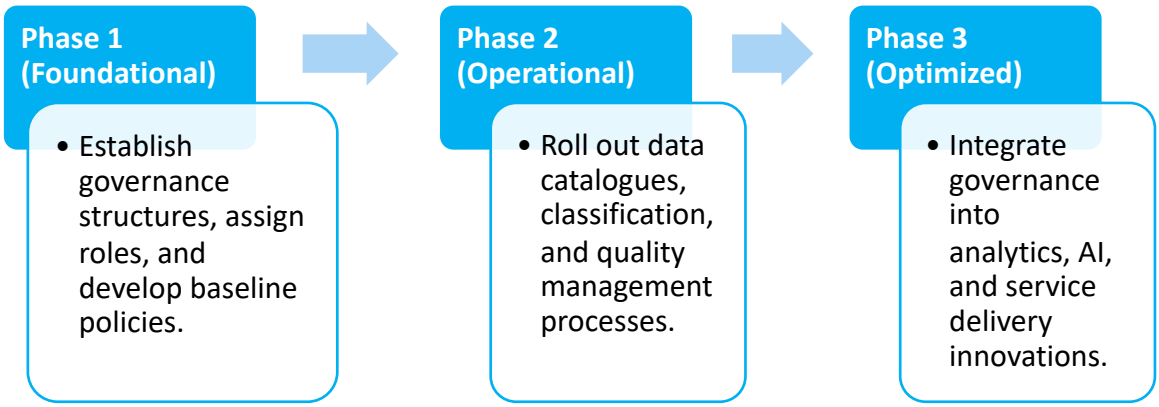

Figure 6: Data Governance Program Roadmap

6.1. Institutional Data Governance Framework

Under the oversight of the central Data Governance Custodian (NISR), each government institution shall develop and maintain a tailored Data Governance Framework aligned with its operational context. This framework acts as a practical guide for embedding governance principles into daily operations through clear policies, processes, and accountability mechanisms.

Key elements of the framework should include:

- **Vision and Objectives:** Defining the institution's vision, goals, and principles for managing data as a strategic asset.
- **Roles and Responsibilities:** Establish decision-making bodies and designate **Data Owners, Data Stewards, Data Custodians, and Data Governance Officers** with clear responsibilities and accountability for ensuring trusted, secure, and well-managed data.

- **Policies, Processes, and Standards:** Document and enforce policies, procedures, and standards covering data classification, quality, sharing, protection, privacy, and retention to ensure consistency across the institution.
- **Measurement and Monitoring:** Set **Key Performance Indicators (KPIs)** and monitoring mechanisms to track data quality, manage risks, resolve governance issues, and regularly report progress to leadership and stakeholders.
- **Technology and Architecture Enablement:** Utilizing tools like enterprise data catalogues, metadata repositories, business glossaries, and data quality systems to enhance data interoperability and consistency of institutional data assets.
- **Communication and Engagement:** Promote continuous communication, awareness campaigns, and training programs to embed governance into institutional culture, strengthen data literacy, and ensure compliance with governance rules.
- **Continuous Improvement**: Regularly review governance practices, update standards, and assess maturity levels to ensure the framework remains effective, relevant, and adaptable to evolving needs and technologies.

6.2. Data Governance Structures, Roles, and Responsibilities

A successful data governance program relies on clearly defined roles, structures, and associated responsibilities to ensure operational effectiveness, accountability, and alignment with national data governance objectives.

Each GoR institution must define and implement its own governance roles, structures, and responsibilities, tailored to its size, resources, and capabilities, while aligning with this framework.

These roles do not necessarily require hiring additional staff; where possible, they can be incorporated into existing positions [9]. However, if resources are allowed, new staff may be recruited. What is essential is that the responsibilities are clearly defined and well-integrated into current functions.

6.2.1. Minimum Governance Components and Roles

The following components and roles to support data governance must be established as a minimum:

Data team
The purpose of this committee is to provide strategic oversight and decision-making for data governance initiatives.

Responsibilities of this team are:

- Approve the institution's Data Governance Framework, policies, and standards.
- Define strategic objectives for data management and data quality.
- Review and endorse key data-related decisions, including access, sharing, and classification.
- Monitor overall compliance with data governance policies and national requirements.

9 Data governance roles have been mapped to existing roles available in GoR institutions in Table 1: Data governance roles mapped to existing roles in GoR

- Serve as the escalation point for unresolved data-related issues and conflicts.
- Promote a culture of data-driven decision-making across the institution.

The team is composed the Chief Data Officer, (serving as Chair), the Data Steward& Governance Officer (serving as Secretary), and representatives of Data Owners, and Data Custodians.

Chief Data Officer (CDO)

The chief data officer leads and coordinates the institution's data governance program.

Responsibilities of CDO are:

- Lead data team and Implement the Data Governance Framework, ensuring alignment with institutional and national priorities.
- Coordinate with Data Owners, Stewards, Custodians, and Governance Officers to ensure roles are effectively executed.
- Monitor data quality, compliance, and performance against KPIs.
- Report governance progress to the Data Governance Committee and institutional leadership.
- Advice on technology and tools needed to support governance processes.
- Lead awareness, capacity-building, and training programs related to data governance.
- Collaborate with NISR and RISA for smooth implementation

Data Owners (Business Accountability)

Data owners provide accountability for datasets and authorize their use.

Responsibilities of the data owner are:

- Define the purpose, usage, and access rights of the data under their ownership.
- Approve data access requests and sharing arrangements.
- Ensure datasets comply with legal, regulatory, and institutional policies.
- Validate data quality reports and take action on critical issues.
- Collaborate with Data Stewards and CDO to resolve governance challenges.
- Participate in strategic planning related to data management.

Data Steward & Governance Officer

Operationalize governance processes and support the CDO in enforcing standards.

Maintain day-to-day quality, consistency, and usability of data.

Responsibilities are:

- Develop and maintain governance policies, procedures, and standards.

- Monitor implementation of governance practices across departments.
- Maintain a registry [10]of Data Owners, and Custodians.
- Conduct periodic governance assessments and report findings to the CDO.
- Facilitate training, awareness, and communication initiatives on governance.
- Support the preparation of institutional data governance performance reports.
- Collaborate with NISR and RISA to enforce data governance guidelines
- Serves as the focal person for data governance
- Provide guidance and training to staff on proper data handling practices.

Data Custodians (Technical Implementation & Security)

Manage the technical infrastructure and ensure secure, reliable data storage.

Responsibilities of data custodians are:

- Maintain databases, data warehouses, and other data systems.
- Ensure data is securely stored, backed up, and recoverable.
- Implement access controls and security measures per governance policies.
- Support Data Stewards in maintaining data quality and integrity.
- Monitor system performance and troubleshoot technical issues affecting data availability.
- Collaborate with CDO and IT leadership to deploy technology solutions that support governance objectives.

Figure 7 Key Roles and Responsibilities

10 A registry is a formal list showing who owns, manages, and technically maintains each dataset.

6.2.2. Mapping data governance roles based on current government roles

For data governance to be effective, it should build on roles and structures that already exist within government institutions. Aligning the framework with current mandates helps avoid duplication, leverages established expertise and ensures smooth integration into existing workflows. This approach strengthens institutional ownership and promotes the consistent application of governance principles across all sectors.

The table below maps roles based on the data governance framework to enhance full and secure access to data.

Table 1: Data governance roles mapped to existing roles in GoR

Data Team's Roles	Current institution roles
Chief data officer	1. Deputy Director Generals 2. Chief Digital Officer (CDO) 3. Chief technology officer 4. Business analyst 5. Head of planning
Data Owners	1. Department Heads / Division Chiefs 2. Program/Project Managers / Project Directors
Data Stewards and Data governance officer	1. Statisticians 2. Data Scientists 3. Data Managers 4. Data analysts
Data Custodians	1. Senior Database Administrators (DBAs)/Specialists 2. Senior System Administrators /Specialists 3. Data Engineers 4. Network Senior Engineers /Specialists 5. ICT Director 6. Senior Software Developer 7. Software Engineers 8. Software Developer 9. IT Specialist

Where governance roles fail to meet their obligations, issues will be escalated from the institutional governance committee to NISR for review. Persistent non-compliance may trigger independent audits and corrective action plans agreed with institutional leadership.

6.3. Adopt and Implement Data Governance Guidelines

Government institutions must adopt and tailor the data governance guidelines developed by NISR and RISA to align with their mandates, legal obligations, and operational realities. These guidelines collectively ensure that data is accurate, consistent, well-documented, properly classified, securely accessible, and effectively managed throughout its lifecycle. By embedding them into institutional processes, government institutions strengthen accountability, improve interoperability, discoverability, and enhance the reliability of data for decision-making, service delivery, and public trust.

6.3.1. Metadata Management guidelines

The first step in governance is understanding your data, identifying what exists, where it comes from, its structure, content, and usage, and creating an inventory of these assets. GoR Institutions must document the full lifecycle of their data, capturing key metadata as recommended by national metadata management guidelines.

With guidance from the central Data Governance Custodian, each institution must:

- Create and maintain a Data Catalogue[6]
- Manage metadata in line with national metadata management standards
- Define and maintain Data Lineage [7] to track the flow of data from the source to use
- Develop a Business Glossary [8] to provide clear business definitions linked to technical metadata

The Data Catalogue and Metadata repository improve data discoverability and interoperability. Data Lineage supports impact analysis, risk assessment, and compliance. At the same time, the Business Glossary ensures a shared understanding between technical and non-technical stakeholders and forms the basis for data quality rules.

6.3.2. Data Classification and Access Management

Following the National Data Classification and access guidelines, GoR institutions must classify data in five levels (Public, internal, confidential, and restricted) based on sensitivity and intended use by ensuring confidentiality, compliance, and privacy protection. Classifications must be applied consistently across systems and documented in the Data Catalogue.

This guideline defines protocols for authorizing, restricting, and monitoring access. Institutions must implement access controls suited to their environment while ensuring transparency, security, and auditability. Responsibility for maintaining these classifications and access records lies with data owners, supported by data stewards and custodians.

6.3.3. Data Quality and Standards guidelines

According to the Data Quality and Standards guidelines, data must be clearly understood (identified, documented, and given explicit meaning) and must remain complete, accurate, timely, and consistent.

11 Data Catalogue is a centralized inventory describing datasets, their sources, owners, quality, and usage.
12 Data Lineage is a documented path showing where data originates, how it moves, and how it changes across systems.
13 Business Glossary is a standardized dictionary of key concepts and definitions, ensuring everyone in the institution understands and uses data in the same way.

Each institution must establish a Data Quality Management Program that:

1. Defines data quality rules and metrics based on business requirements
2. Measures data against these rules
3. Remediate quality issues at their source
4. Follows the required data standards

Automated quality checks and ongoing measures should be implemented to track improvements over time. Data Stewards, working with Custodians, must identify root causes of quality issues, implement corrective actions, and provide regular reporting to prevent risks to decision-making and service delivery.

6.3.4. Data Incident Management, Retention, and Security Guidelines

The guidelines on data incident management, retention and disposal, and data security and privacy outline measures to ensure data is protected, managed, and secured effectively. Institutions should have clear procedures for identifying, reporting, and addressing data breaches, corruption, or loss, ensuring rapid action to limit damage and maintain operations. Data retention schedules must be defined to determine how long different types of data are kept, with secure and irreversible disposal methods applied once data is no longer needed. Security measures should match the sensitivity of the data, using tools such as encryption, controlled access, and regular security audits to prevent unauthorized access, misuse, or disclosure. Together, these practices enhance data integrity, compliance, and trust. GoR institutions must adopt these guidelines to align with the institutional context.

6.3.5. Interoperability and Data Integration

Building on the foundational data governance policies, metadata standards, and data classification principles outlined in their related guidelines, government institutions will take specific steps to achieve interoperability and data integration.

Institutions will adopt common data standards and protocols that enable technical compatibility and semantic consistency across systems, facilitating seamless data exchange and combined analysis. The use of unique identifiers on people, businesses, and locations will be enforced to accurately link records from diverse data sources, as part of the National Data Infrastructure initiatives.

Formalized data-sharing agreements will define roles, responsibilities, access permissions, and data protection safeguards to maintain privacy and security during integration processes.

Technical teams will collaborate to develop or enhance interoperable platforms and services that support data discovery, access, and harmonization, leveraging metadata frameworks. Institutions will participate in coordination mechanisms to monitor interoperability progress and address integration challenges, ensuring alignment with the broader national digital transformation goals.

6.3.5. Data Lifecycle Management

Aligned with the data quality management principles and data security discussed in the guidelines, Data Lifecycle Management should be operationalized through detailed policies and procedures addressing data creation, storage, archival, retention, and disposal.

Government institutions will establish clear retention schedules consistent with legal requirements and

operational needs, ensuring data is maintained only as long as necessary. Data classification categories and access control guide the appropriate handling of data at each stage of the data lifecycle.

Secure storage and archiving solutions will be implemented to preserve data integrity and enable retrieval for compliance, research, and administrative purposes. When data reaches the end of its retention period, institutions apply secure, verifiable disposal methods in line with privacy protections and risk management approaches. Periodic audits and compliance reviews will assess adherence to lifecycle policies and identify areas for improvement. The institution should conduct capacity-building initiatives to ensure that staff are equipped with the knowledge and skills to manage data responsibly throughout its lifecycle.

6.4. Regulatory Compliance

Regulatory compliance is a fundamental component of the data governance program and must be fully integrated into all data governance activities. A primary objective of data governance is to ensure adherence to all applicable sector-specific and national laws governing the collection, storage, protection, and use of data.

In particular, compliance with Law N°. 058/2021 Relating to Data Protection and Privacy (DPP) and the Statistical Law (Law No. 45/2013) is mandatory for all government institutions. These laws set the legal framework for responsible data management, confidentiality, privacy, and the production of official statistics.

By implementing the governance structures, roles, and processes outlined in this framework, institutions establish a solid foundation to meet privacy, data protection, and statistical reporting requirements while also realizing the broader benefits of effective data governance.

Each institution's data governance program must be tied to measurable KPIs, such as % of datasets classified, % of metadata catalogued, and % of data governance guidelines implemented, % of data quality improved. These KPIs should align with both institutional IMIHIGO and national data governance performance indicators.

6.5. Risk Management in Data Governance

Risk management is a foundational element of effective data governance within GoR institutions. It involves proactive identification, assessment, and mitigation of risks that could compromise data integrity, confidentiality, availability, and compliance with legal and regulatory requirements. Through regular data audits, security assessments, and continuous monitoring, institutions can detect vulnerabilities and threats early, enabling timely intervention.

Implementing robust technical controls such as encryption, access restrictions, and secure data handling procedures is essential to safeguarding sensitive information. Clear incident response protocols must be established to ensure prompt reporting, management, and resolution of data breaches or quality issues. Equally important is fostering a risk-aware culture through ongoing training and awareness programs that empower staff to recognize and manage risks effectively.

By embedding risk management practices within the data governance framework, Rwanda's government institutions will enhance data security, uphold citizen privacy, maintain compliance with national laws, and reinforce public trust in government data assets.

6.6. Change Management and Capacity Building

The successful adoption and long-term sustainability of data governance within government institutions

depend on both effective change management and robust capacity building. The leadership of each GoR institution should lead and facilitate change management within its institution. This role focuses on preparing institutions and personnel for the transition to structured data-governance practices by clearly communicating benefits, securing leadership commitment, and engaging stakeholders at all levels.

Each institution should implement structured change management plans to guide staff. The roadmap should include awareness campaigns to build staff buy-ins, pilot projects to demonstrate quick wins. The plan should feedback mechanisms to refine governance processes and should also promote a culture that recognizes data as a strategic asset. Institutional leadership must champion data governance, allocate the necessary resources, and model expected practices.

The National Institute of Statistics of Rwanda (NISR), together with development partners, will coordinate and facilitate capacity-building programs to strengthen staff skills and knowledge, tailored to the responsibilities of the different roles in the data-governance program.

Capacity building will follow a structured roadmap: introductory training for all staff in Year 1; advanced certification for data Owners, Stewards, Custodians, and data governance Officers by Year 2; and continuous professional development aligned with evolving international standards thereafter.

Every GoR institution should encourage and facilitate ongoing professional development to build staff capacity, ensuring employees remain proficient amid evolving technologies, international standards, and regulatory requirements.

Chapter 7

Monitoring, Evaluation, and Continuous Improvement

To ensure that Rwanda's Data Governance Framework remains effective, relevant, and aligned with national development goals, it is essential to establish a robust system for monitoring, evaluation, and continuous improvement. This system enables government institutions to track progress, identify gaps, and adapt governance practices based on evolving needs, technology, and stakeholder feedback.

7.1. Data Governance and Management Maturity Model

The Government of Rwanda will adopt a combined Data Governance and Data Management Maturity Model to guide public institutions in the progressive implementation of robust data practices. This integrated framework enables institutions to systematically evaluate both governance structures and operational data management capabilities, ensuring that leadership, policies, roles, and processes are aligned with national priorities and contribute to effective, data-driven decision-making.

The model consists of five maturity levels, with each level representing a stage of evolution in governance and management. The levels are interdependent: strong governance structures provide the foundation for effective data management, while high-quality management practices validate and reinforce governance policies.

- **Level 1: Initial**

  At this stage, institutions do not have formal structures or clear processes for managing data. Roles and responsibilities are unclear, and there are no consistent policies or rules in place. Data is managed reactively, often in isolation by different teams, leading to fragmented and inconsistent practices. Data quality is generally poor, and little or no documentation or metadata is maintained. Without proper governance oversight, management decisions rely on uncoordinated and unreliable data.

- **Level 2: Developing**
  Institutions begin to recognize data as a strategic asset. Basic governance policies are introduced, and roles such as Data Owners, Data Stewards, and Custodians are assigned. Leadership engagement increases, and initial efforts toward data classification and inventories are underway. Operationally, some processes are defined, metadata is partially captured, and periodic data quality checks are performed. Governance improvements at this level enable early structuring of data management processes, but practices remain inconsistent and require further institutionalization.

- **Level 3: Defined**
  At Level 3, formal governance frameworks are operational, with a functional data governance committee, documented policies, and clear responsibilities. Data governance mechanisms provide oversight for compliance, risk management, and stakeholder engagement. On the management side, data lifecycle processes are standardized, data quality is regularly monitored, metadata and classification registers are maintained, and partial interoperability across systems is achieved. Governance at this level directly supports structured and repeatable operational data practices, ensuring consistency and reliability.

- **Level 4: Managed**
  Data governance is embedded into institutional operations. Leadership actively promotes ethical and compliant data use, allocates resources, and fosters a culture that values data as a strategic asset. Governance policies are consistently applied, and institutional risk management is operational. Operationally, automated processes are implemented where feasible, administrative data is systematically used for official statistics, and data is accessible, interoperable, and secure. Management practices at this level reflect the strength of governance structures, demonstrating alignment between policy, oversight, and operational execution.

- **Level 5: Optimized**
  Level 5 represents a state of continuous improvement and innovation. Governance mechanisms drive strategic use of data, ethical leadership, and institutional excellence. Institutions actively evaluate and refine policies, benchmark performance, and are recognized for exemplary practices. Data management is fully operationalized, leveraging advanced analytics, AI, and digital tools on well-governed data. Processes are continuously improved, interoperability is seamless, and data effectively support national development priorities. At this stage, governance and management maturity are fully aligned, creating a sustainable and innovative data ecosystem.

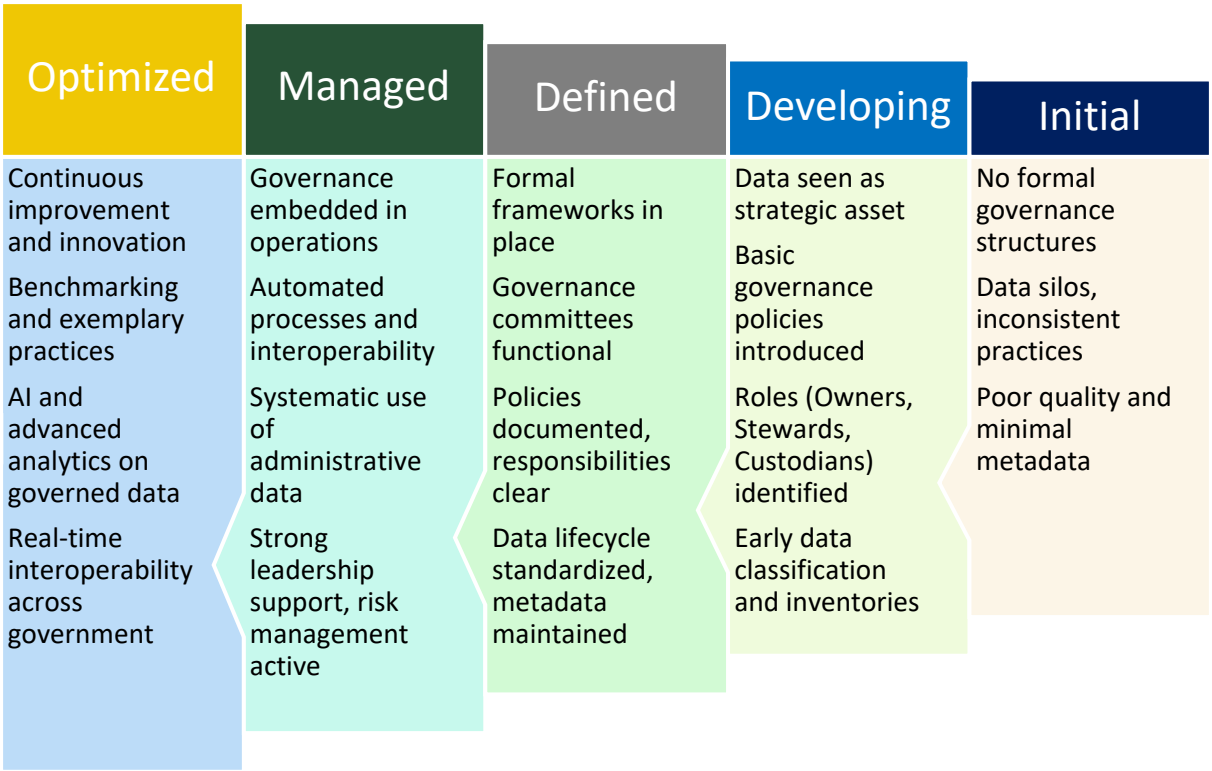

Figure 8: Data Governance and Management Maturity Model

Findings from maturity assessments must directly inform updates to data governance policies, capacity-building priorities, and institutional targets. NISR will publish recommendations alongside the national maturity report to ensure continuous learning and adaptation.

Assessment Process:
Each institution will conduct an annual self-assessment against this maturity model. The National Institute of Statistics of Rwanda (NISR) will validate these assessments through peer reviews and audits. The consolidated results will be published in a National Data Governance and Management Maturity Report, which will guide policy refinement and capacity-building initiatives.

To strengthen the credibility of assessments, NISR will provide training, templates, and technical support to help institutions conduct robust self-assessments. Development partners may be engaged to support independent reviews and build advanced evaluation capacity.

Over time, Rwanda will benchmark its maturity levels and KPI results against international standards (e.g., OECD, DAMA, World Bank) and peer countries to position itself as a regional leader in data governance.

7.2. Key Performance Indicators (KPIs)

To measure progress and effectiveness, Rwanda will use Key Performance Indicators (KPIs) aligned with national priorities and the objectives of the Data Governance Framework. These KPIs provide clear, measurable benchmarks across the critical dimensions of data governance. Implementation of data governance must be integrated into the annual GoR institutional performance contracts (IMIHIGO). For staff with data responsibilities, relevant KPIs should be reflected in their institution's IMIHIGO and, where appropriate, in individual performance agreements.
To ensure transparency and efficiency, institutions will use a standardized national monitoring dashboard managed by NISR. This platform will automate KPI tracking, allow real-time reporting, and provide both government and citizens with visibility into data governance progress.

The KPIs will cover domains including data quality and standards, metadata, data classification, and access, data sharing, and use of administrative data. The KPIs will also cover topics like interoperability and infrastructure, capacity building and innovation, governance and maturity, security and privacy, and monitoring and reporting performance. Each KPI will be defined with a clear numerator and denominator, a reporting frequency, a designated owner, and a data source. Institutions will report KPI data quarterly; NISR will consolidate and analyse results to produce an annual national report. Post-assessment stakeholder engagements will support learning and refinement, and targeted support will address identified gaps. Data governance guidelines and KPI definitions will be reviewed every two years. An annual Data Governance Excellence Award will recognise outstanding institutions based on KPI achievement, data management maturity improvements, and adoption of ethical and secure data practices.

Chapter 8

Conclusion

The data governance framework for the Government of Rwanda defines how data should be managed to maximize its value as a strategic asset, benefiting not only individual government institutions but the nation. Based on international standards and best practices, it provides a unified approach to data governance across all government entities.

To achieve this, each institution must implement the core principles, roles, structures, processes, and mechanisms outlined in the framework. They will be supported by NISR -acting as the central Data Governance Custodian), responsible for providing guidance, standards, templates, and ongoing assistance. Strong data governance is founded on effective data management and risk management capabilities, including data security, privacy protection, metadata management, and data quality assurance.

By adhering to these principles and guidance, government institutions will collectively increase the value of Rwanda's data assets, contributing to national development goals and positioning the country both as a smart nation and regional leader in digital innovation. Ultimately, this will contribute to building a society where Rwandans live in an environment informed by trusted data.

Chapter 9

Annex

This Annex is designed as a practical reference for policymakers, data governance officers, and technical staff. Each table and definition support specific sections of the framework; for example, Table 2 aligns with Section 6.2 on roles, and Table 5 aligns with Section 7.2 on KPIs. Institutions should use this Annex as a toolkit to operationalize the framework.

9.1. A diagram illustrates a data governance framework

The diagram below illustrates a sample framework that provides a blueprint for all the components of a data governance program:

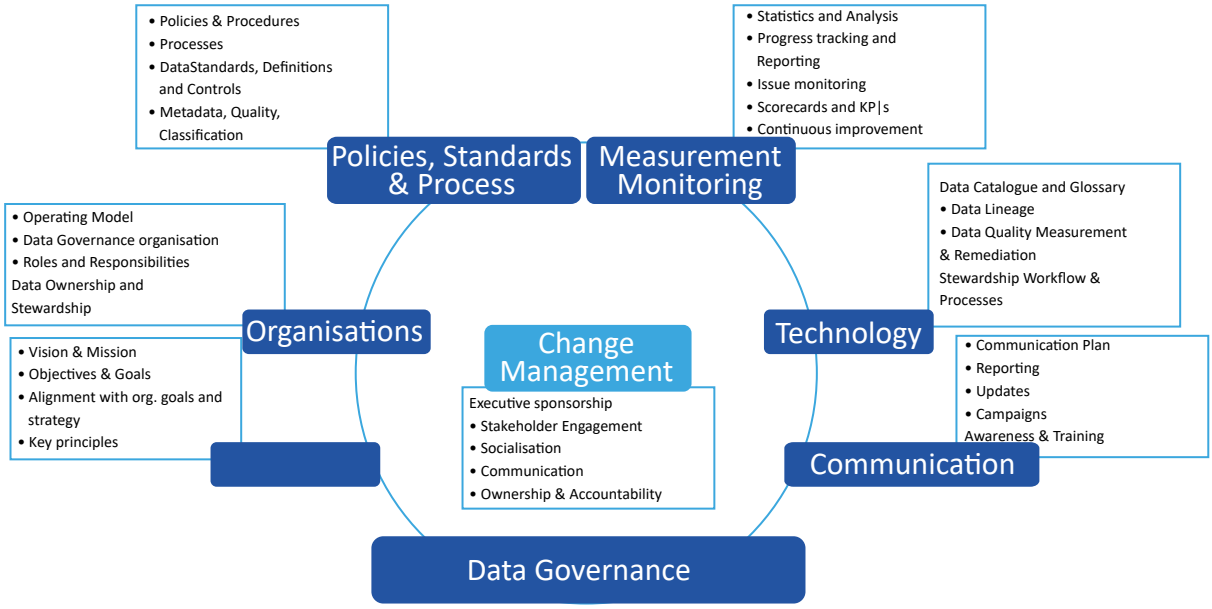

Table 2: Primary Data Governance Terms and Definitions

Term	Definitions
Business Term	A definition of how data is used within the 'business' or functional areas of the organisation. An example of a business term could be 'National Identifier' with a description of what that means to the organisation, what its format should be and what access restrictions are set on it. A business term and the associated data elements (technical definition) in the data catalogue are linked together to create a business glossary, with the goal of creating a common understanding of data.
Critical Data Elements	CDEs are data elements that are critical to the success of a specific area or domain. They are most often associated with Master Data domains such as Party, Product etc. and will, if their quality and usage are not properly managed, pose the biggest risk or have the most financial impact on the organisation. Data elements (such as National Identifier, Name, Address) that are classified as Personally Identifiable Information are also a good example of CDEs. Identification of CDEs is essential to managing the scope and focus of data governance operations to ensure the proper governance of data that has the most impact or is most important to the organisation
Data Governance	The term 'Data Governance' refers to "the collection of practices and processes which help to ensure the formal management of data assets within an Organisation" (DAMA DMBoK).

Data Governance Program	The program for implementation and embedment of data governance as a key strategic capability within an organisation. The program is formally managed as such and is sponsored at an executive level.
Data and Information	In this document the terms 'data' and 'information' are used interchangeably and refer to the data assets of an organisation, which must be governed to ensure their integrity, quality, completeness, and availability.
Data team	A committee comprising one or more executives or senior management, such as a Minister or Director General. Sometimes these are known as Executive Data Owners or Executive Sponsors. They are ultimately accountable for the value of data as an organisational asset and its use to achieve ministerial objectives. They oversee the implementation of data governance activities, and each member will be responsible for the establishment of data ownership and data stewardship within their area of oversight. The Data Sponsor must • Endorse key strategic decisions, e.g., what data is collected, how is it used to achieve organisational objectives, etc. • Provide oversight and direction to Data Owners in the organisational areas under their mandate • Act as a key stakeholder for data governance activities including approving funding
Data Owners	A Data Owner is a person in an oversight or management role, typically at the head of a department or Director, Division Manager, or similar level within a government institution, who is accountable for the governance of specific sets of data that relate to the functional area within which they operate. Such data sets will be clearly defined according to their organisational responsibility as part of the data governance program. The data owner acts under the authority and on behalf of the executive Data Sponsor and the Data Governance committee. The data owner understands the purpose or goal of the data and is accountable for ensuring the quality and correctness of the data and mitigating any risks to the data. The data owner is responsible for ensuring that data stewards in their area of oversight can fulfil their roles, particularly in respect of metadata management, data understanding, data quality management and data privacy.
Data Custodians	A person, typically from the Information Technology division, who has the technical and data expertise to assist data stewards to fulfil their functions, particularly as these relate to understanding, quality, and appropriate use of data. Data Custodians will be assigned according to their areas of expertise, for example at a system or data architecture level.
Data Stewards	Data Stewards are responsible for curating data in their domain. Among their responsibilities are: • Working with Data Owners to define Critical Data Elements • Working with Subject Matter Experts across IT and Business functions to define the appropriate standards and meaning of data terms • Working with Data Custodians to ensure the collection of relevant metadata for the critical data in the data catalogue and data dictionary • Working with Data Owners, process owners and SMEs to create business terms and develop the Business Glossary • Working with subject matter experts, including process owners, to define the business rules and expectations for data • Working with data custodians and technical experts to ensure the definition of data quality rules and the implementation of these • Working with the reporting and BI or team or data tools experts (depending on which tools are implemented for data governance) to ensure that that relevant operational reports are implemented for metadata and data quality management • Liaising with other Data Stewards to deal with any conflicts or duplications amongst Business Terms across the enterprise • Act as a review and approval gate for changes to, or additions of Business Terms • Ensuring that appropriate data assets are tagged with relevant Business Terms in a meta data repository (Data Catalogue)

9.2. The Relationship Between Data Management and Data Governance

DAMA (the Data Management Association) International defines data governance as "the planning, oversight, and control over management of data and the use of data and data-related sources".
For data to be of value to any organisation, it must be well managed. Data Governance cannot exist without these basic disciplines required to manage data effectively and will strengthen such disciplines by improving the understanding, quality, and value of data.
The diagram below, commonly known as the 'DAMA Wheel,' illustrates the 10 primary data management functions, capabilities, or disciplines, with data governance at the centre as the 11th function which provides oversight to all other activities:

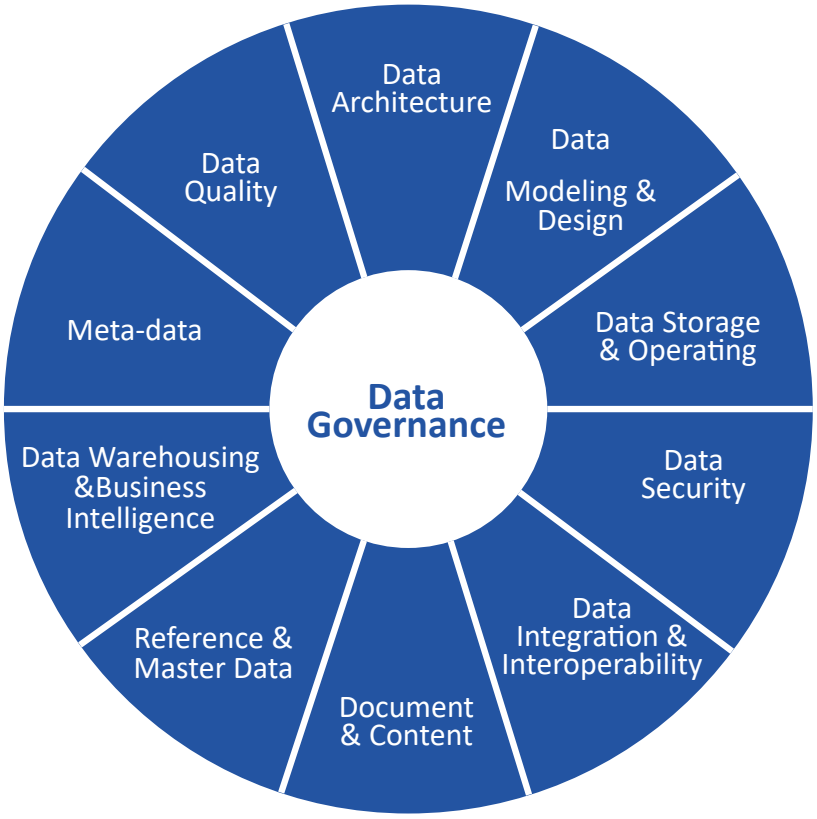

Figure 1 – The DAMA Wheel of Data Management Knowledge Areas

Each of the disciplines or knowledge areas illustrated on the outer part of the wheel are briefly explained below. Each of these may exist to varying degrees of capability maturity within each organisation, depending on the nature of its operational activities.
When establishing a data strategy and a strategy for data governance and procuring the appropriate tools for execution thereof, integration with and support of each of the above facets of data collection, management, archiving, and use should be considered.
The foundational or critical capabilities for data governance are:

- Data Risk Management – Security, Privacy and Compliance
- Metadata Management
- Data Quality Management

Table 3: Data Management Disciplines

Knowledge Area / Discipline	Description
Data architecture	The overall structure of data and data-related resources as an integral part of the enterprise architecture
Data modeling and design	Analysis, design, building, testing, and maintenance of data
Data storage and operations	Structured physical data assets storage deployment and management
Data security	Ensuring privacy, confidentiality, and appropriate access
Data integration and interoperability	Acquisition, extraction, transformation, movement, delivery, replication, federation, virtualisation, and operational support
Documents and content management	Storing, protecting, indexing, and enabling access to data found in unstructured sources and making this data available for integration and interoperability with structured data
Reference and master data	Management of shared data to reduce redundancy and ensure better data quality through standardised definition and use of data
Data warehousing and business intelligence	Management of analytical data processing and enabling access to decision support data for reporting and analysis
Metadata	Collecting, categorizing, maintaining, integrating, controlling, managing, and delivering metadata
Data quality	Defining, monitoring, maintaining data integrity, and improving data quality

Table 4: Monitoring, Evaluation, and Continuous Improvement Framework

Component	Description	Implementation examples
Data Governance Maturity Model	A structured framework to assess the level of data governance implementation across government institutions, identifying strengths, weaknesses, and gaps.	Use a 5-level maturity model (Initial, Developing, Defined, Managed, Optimized). Each ministry and agency will be periodically assessed on four dimensions (People, Process, Technology, and Measurement) to measure progress in implementing data governance.
Level 1 – Initial	No formal governance, data is siloed, inconsistent, and uncoordinated.	Most administrative data sources are not standardized; minimal integration for official statistics.
Level 2 – Developing	Some governance initiatives exist but lack coordination and clear accountability.	Basic metadata standards adopted; pilot initiatives for unique identifiers underway in select sectors.
Level 3 – Defined	Governance policies and frameworks are documented; roles and responsibilities are clear.	Implementation of national metadata standards and unique identifiers (e.g., national ID, business registration number) across core datasets.

Level 4 – Managed	Data governance processes are consistently applied, monitored, and improved.	Integration of administrative data into official statistics is systematic, supported by the Rwanda National Data Infrastructure.
Level 5 – Optimized	Governance is fully embedded in operations; continuous improvement driven by analytics and feedback loops.	Real-time data integration, AI-powered analytics for decision-making, and data sharing across government with full compliance to laws and standards.
Key Performance Indicators (KPIs)	Quantifiable metrics to monitor the effectiveness of the Data Governance Framework and ensure alignment with national strategies.	KPIs will be tracked annually and reported to the Data Governance unit NISR.
KPI 1	% of government institutions with an implemented Data Governance Policy aligned with the national framework.	Target: 100% by 2028.
KPI 2	% of administrative datasets integrated into the National Data Infrastructure with unique identifiers.	Target: 80% by 2028.
KPI 3	% of data quality improvement projects completed annually.	Target: Minimum of 3 per year.
KPI 4	% of metadata-compliant datasets in line with national and international standards	Target: 90% by 2028.
KPI 5	User satisfaction score for access to and usability of official statistics from administrative data.	Target: ≥ 85% satisfaction rate by 2027
KPI 6	The number of capacity-building sessions on data governance is conducted annually.	Target: At least 4 sessions per year.
Continuous Improvement: Feedback & Adaptation	Regular review of performance data, stakeholder feedback, and technological trends to refine governance practices.	Annual policy and standards update, integration of emerging technologies like AI for data quality and analytics, and alignment with evolving national policies.

Table 5: Key Performance Indicators (how success will be measured)

Role	Key Performance Indicators (KPIs)
Chief Data Officer (CDO)	• % of data initiatives aligned with institutional and national strategies • % of critical datasets integrated into governance framework • % improvement in data quality and availability (year-over-year) • % of strategic projects/policies informed by governed data • % of allocated budget utilized effectively • Stakeholder satisfaction score on data accessibility, quality, and governance • Number of cross-institutional data sharing agreements facilitated • Frequency/quality of governance performance reports to senior management and regulators
Data Governance Officer (DGO)	• % of units with designated governance roles (Owners, Stewards, Custodians) • % of policies, standards, procedures documented and disseminated • % compliance with governance policies in reviews/audits • Number of training/awareness sessions delivered • % of governance issues/escalations resolved through governance processes • Timeliness of submitting governance performance reports to NISR • % of governance committee recommendations implemented on time
Data Owner	• % of datasets with clearly assigned Owners • % of data access requests approved/rejected within agreed timelines • % compliance with legal, policy, and regulatory requirements • % of decisions supported by owned datasets • Frequency of ownership/policy reviews completed on schedule
Data Steward	• % of datasets with complete, up-to-date metadata • % of data issues resolved within SLA • % of assets with standard definitions and rules applied • % of datasets meeting quality thresholds (accuracy, completeness, timeliness, consistency) • Number of successful quality audits/checks passed • % of datasets with approved classification/sensitivity labels
Data Custodian	• % system uptime and dataset availability • % of access rights granted/revoked within SLA • % of datasets with successful backup and recovery tests • % of security incidents detected/resolved within SLA • Compliance rate with cybersecurity/data protection standards • % of systems covered by disaster recovery and business continuity tests

Each component of this Annex is directly linked to operational sections of the framework: Tables 2 and 3 support Section 6 (program establishment), Table 4 supports Section 7 (maturity model), and Table 5 supports Section 7.2 (KPIs). Institutions should always consult these annexes when implementing corresponding parts of the framework.