Data Governance FY25-26 Roadmap

October 2024

water.org®

Table of Contents

Introduction

Data governance refers to the management of the availability, integrity, security and use of data in an organization. It is also a structure that establishes responsibility for data, organizing functional experts or business domains to collaboratively and continuously improve data quality and use. It does this through the systematic creation and enforcement of policies, roles, responsibilities, and procedures.

This framework or roadmap outlines Water.org's data governance structure, data management operating procedures, and key stakeholders and their role in ensuring data is suitable for operations, management, planning, and budgeting.

By implementing elements of data governance outlined in this framework, Water.org aims to reduce risks, improve data quality, and enhance operational decision-making.

Data Governance Roadmap

Water.org's vision is to establish a robust data governance framework that empowers our organization to harness the full potential of our data assets. We aim to foster a culture of data excellence where data accuracy, compliance, and security are the cornerstones of our operational effectiveness and strategic decision-making.

Data governance boosts efficiency and enhances communication by standardizing data practices across various regions, countries, departments, or functions within an organization. This uniformity in data definitions and rules ensures consistency. Without shared definitions, organizations and stakeholders might misinterpret or misunderstand data. Receiving different answers from separate departments undermines trust and confidence in the data's reliability and integrity.

Data governance can help reduce costs, including:

- Time spent hunting missing information
- Redundant data entry
- Decreased productivity
- Data clean up
- Difficulty in making decisions due to incomplete or inaccurate data
- Inability to conduct meaningful evaluations
- Staff morale
- Time spent making repetitive decisions because policy is not clear

Intended Outcomes:

- A common vision for more effective data usage in support of organizational goals and strategic initiatives
- Improved data quality
- Improved understanding of data collected, reported, and used by each program and the organization as a whole
- Increased consistency and reduced redundancy of data collected across the organization
- Security, regulations and compliance and privacy requirements of data are maintained and enforced
- More effective communication and coordination among departments – organization-wide responses to critical data issues
- Decreased staff burden (over time)

FY25 & FY26 Strategic Priorities

Over the next two years, we aim to collaborate with various departments to document their data structures, identify Critical Data Elements (CDEs) and metadata, and expand our Data Governance Council's operations.

Continue to provide basic training for the organization as well as more in-depth training for council members and leadership. We will also establish processes to ensure the working groups or primary business users of the data and systems are trained and knowledgeable of data dictionary and data lineage.

We will differentiate discussions for leadership versus those for the Data Governance Council to clarify and define the process for data request or data changes, with a better understanding of data lineage and implications. Additionally, we will work on streamlining processes for system and data updates, such as year-end close activities involving Project IDs and grants or funds.

Our strategy will also focus on long-term solutions for data management, which may include implementing a data dictionary or a centralized data warehouse to facilitate quick access for reporting.

Furthermore, we are undertaking parallel projects and initiatives to establish comprehensive policies and regulations that the Data Governance Council will enforce. These policies will cover areas such as Data Privacy, Data Security, and Data Retention and Lifecycle Management. The preliminary work we are currently conducting will aid in identifying relevant data types, informing the development of these policies.

Data Governance Roles & Responsibilities

There are several essential roles in data governance that contribute unique responsibilities and expertise towards effective data governance. Part of our work over the next two years will be making sure that staff understand what role they are in and what their responsibilities are in ensuring data is handled properly and securely across Water.org.

Here is the list of the data governance roles and responsibilities that will be relevant to our organization:

Strategic Level

Executive Sponsor(s)	• Provide guidance on strategic priorities and vision • Mediate cross-enterprise escalations from Data Governance Council • Accountable for funding, program, and monitoring progress

Strategic & Operational Level

Data Governance Council	• Establish, document, and enforce organization-wide data standards, policies, and processes. • Identify, prioritize, and support the resolution of critical data issues that affect the quality and use of data. • Hold data stewards accountable for participating in the data governance program and adhering to the Data Governance Policy.

Data Governance Lead	• Design and develop Data Governance roadmap and provide reports regarding progress from time to time. • Serve as a single point of contact for data quality and governance. • Serve as a liaison between the business and both its functional and technical areas, ensuring the protection of sensitive and confidential data. • Lead resolution for end-to-end issues regarding Data Governance that may arise from different departments in the organization.

Operational Level

Data Owners	• Ensure data collection and reporting are properly authorized. • Collaborate with the data stewards to resolve or inform Data Governance Council of the issues. • Work with data stewards to prioritize and inform them of critical data issues in their functional area to be brought to the Data Governance Council. • Assist in communication and education of staff in key areas (Data Governance, Data Quality, etc.)
Data Stewards	• Data Documentation: maintaining metadata and data dictionaries • Attend and participate in scheduled Data Governance Council meetings, as required. • Issue Resolution: Report to the Data Governance Council regarding data issues, new data regulations, and new policies affecting data. • Communicate with their business domain or functional area teams regarding activities and decisions of the Data Governance Council. • Support and advocate data management and governance practices to staff. • Data Security and Access Control: managing data security and defining who can access and modify data and identify opportunities to share and re-use data. • Data Quality Management: ensuring data accuracy, completeness, and consistency.
Working Groups	• Serve as subject matter experts within a specific data domain, consisting of business and technical resources • Support owners and stewards to execute projects and resolve issues within specific data domain

Data Governance Council

In late FY24, Water.org established a **Data Governance Council** to serve as a governing body responsible for the data governance of the organization. Since data governance is a process of continuous improvement, the Data Governance Council is tasked with evaluating and refining existing data governance policies and procedures, both regularly and in response to problems that arise.

Key responsibilities of the Data Governance Council include:

- Develop and implement the overall organization-wide Data Governance strategy
- Establish, document, and enforce organization-wide data standards, policies, and processes.
- Identify, prioritize, and support the resolution of critical data issues that affect the quality and use of data.
- Hold data stewards accountable for participating in the data governance program and adhering to Data Governance policies in effect.

The Data Governance Council meets monthly, and in FY25 has a specific focus on Finance data management to ensure a successful launch of the new accounting software (NetSuite) on October 1, 2025.

A list of the current Data Governance Council members may be found on the Data Governance Sharepoint site. Staff are welcome to email the Data Governance Council with specific requests and/or questions at DataGovernance@water.org.

Data Governance Principles

As we build out our data governance policies and processes, we will be guided by a set of specific guiding principles to ensure consistency, accuracy and security.

- **Governance and Transparency**
  - o Governance should increase transparency, trust, understanding, and speed.
  - o Give all stakeholders ways to add knowledge and improve data assets.

- **Business Problems and Analytics**
  - o Start with the business problems and analytics questions you have today.
  - o Analytics is valuable while it's happening, not just when it's 'done'.

- **Iteration and Improvement**
  - o Iterate quickly to build better habits and get to value faster.
  - o Make documentation easy and iterative or it won't happen.

- **Collaboration and Connectivity**
  - o One person's work should help everyone else's.
  - o Keep people, data, docs, and analysis connected and accessible from the beginning.

- **Methodology and User Experience**
  - o Promote good statistical and scientific methods.
  - o Make the user experience twice as good as the products and practices it competes with to earn adoption.

Data Governance Policies & Procedures

Over the next two years, we will be prioritizing foundational work, which will involve reviewing and updating existing policies, developing new ones where needed, and introducing new processes to enhance data management, and fostering a culture of data ownership.

This section explores various elements of data governance that we will be working on in FY25 and FY26, noting what already exists in terms of policies and procedures, and what will be developed or updated to ensure successful implementation.

Data Definitions

Data definitions and a data dictionary are essential for an organization's data governance and operational practices. They enable standardization, quality control, data integration, lineage tracking, stewardship, and compliance. Currently, we are using Excel spreadsheets to identify critical data elements across various domains and systems. As we develop our strategy and expand our capabilities, we will explore alternative

systems or methods to store and share data definitions organization wide. This approach will enhance data understanding and facilitate quicker, more efficient reporting.

Critical data elements (CDE) are the data that is critical to an organization's success in a specific business area (line of business, shared services, or group function), or the data required to get the job done. This includes data tied to medium and long-term business goals and sensitive data (Personal, Regulatory, Confidential, Risk). The following list is intended as an example but is not considered as a comprehensive list:

- **Donor Information** including contact details, donation history, lead metrics and engagement records.
- **Legal Data** including information related to compliance, tax, and regulatory compliance protecting the business.
- **Financial Records** including income statements, balance sheets, and cash flow statements.
- **Program and Project Data** including information on various programs and projects, such as budgets, expenditures, outcomes, vendor or consultant data, and impact metrics.
- **Grant Management Data** including details on grant applications and approvals.
- **Employee Data** including employment records or job history, personal information, etc.

Metadata describes individual data elements or, simply, is 'data about data' and provides understanding that unlocks the value of data. These are typically elements that the average user does not see, but which describe the relationships between data fields, technical information, who can access the data, and who created it.

- **Business Metadata** describes data from a business point of view. For example, decisions for a data element based on business purpose or functionality. For example, the Revenue Recognition Protocol Naming Conventions for Project IDs.
- **Technical Metadata** is information about the applications, tools, and systems supporting a data management solution. For example, data lineage, source of truth, or data format.
- **Operational Metadata** is information about the process that manipulates and moves data throughout. For example, manual csv or excel manipulations done before uploading into the next system.

Relationship data describe the relationship between entities or objects. Most systems use relational databases. The relationship data (known as keys) link to the many tables that make up the database.

Data quality standards

Data quality standards are essential for effective quality control. Clear definitions set the criteria for evaluating data quality, allowing organizations to assess the accuracy, completeness, and relevance of each data element. We plan to develop a procedure that integrates these quality specifications into our data dictionary. This will establish standards for data formats, naming conventions, metadata, and data models, ensuring consistency across all systems.

Data Security

We plan to develop a Data Security policy, which will be important for safeguarding sensitive information, ensuring compliance, managing risks, and supporting data governance initiatives. It will identify potential security risks and outline strategies for mitigation, enhancing the organization's overall risk management framework.

By establishing clear security protocols and procedures, the policy will promote consistent practices across the organization, minimizing the likelihood of errors or oversights. Additionally, a strong data security policy will align with data governance objectives, ensuring that data is managed securely and responsibly throughout its lifecycle. Compliance with laws and regulations (e.g., DPDP, GDPR, CCPA) is also critical, and a robust policy helps meet these requirements, reducing the risk of legal penalties.

Data Privacy

The development of a data privacy policy will be critical for compliance, risk management, trust-building, and supporting overall data governance, ensuring personal data is managed responsibly. It will provide clear guidelines for employees on handling personal data, minimizing errors and clarifying responsibilities. Many jurisdictions have laws governing data privacy (e.g., DPDP, GDPR, CCPA), and a robust policy will help ensure compliance, reducing the risk of legal penalties and protecting the organization's reputation.

The policy will establish protocols for collecting, using, and storing sensitive information, thereby safeguarding individuals' privacy rights. Additionally, a well-defined privacy policy identifies and mitigates risks related to data breaches and unauthorized access, strengthening the organization's risk management framework. Transparency in data handling practices fosters trust among customers, partners, donors, and stakeholders, demonstrating the organization's commitment to protecting personal data.

Document Retention and Lifecycle Management

A comprehensive Document Retention and Lifecycle Management Policy is essential for regulatory compliance, outlining how long data should be retained and the methods for its disposal. This not only helps organizations avoid legal penalties but also safeguards their reputation. By reducing unnecessary data storage, the policy mitigates risks associated with unauthorized access and breaches, ultimately enhancing data security.

Furthermore, this policy will promote operational efficiency by streamlining data management processes and improving data quality through regular reviews and timely disposal of outdated information. This ensures decision-making relies on current, accurate data while reducing risks related to sensitive information exposure.

Currently, we have a [Record Retention Policy and Schedule](#) for the US in place, but we are committed to developing a more comprehensive policy that encompasses all data types, including digital. This effort will be crucial for responsible data management throughout its lifecycle.

Security Incident Handling and Management

The Security Incident policy and procedures will guide the organization how to respond to data privacy incidents, ensuring that the organization can act swiftly and effectively to mitigate potential harm. An incident management policy is essential for effective data governance as it enables rapid response, mitigates risks, ensures compliance, fosters continuous improvement, facilitates stakeholder communication, and promotes employee awareness.

Please refer to our existing policy, [Security Incident Handling Policy and Procedure,](#) for our issue resolution and data breach response.

Training and Awareness

Training and awareness are essential for effective data governance, security, privacy, and incident management. They equip employees with the knowledge and understanding of policies and best practices,

helping them recognize their roles and responsibilities in protecting, using, and sharing data. This proactive approach shares accountability, mitigates risks, reduces errors, and ensures compliance with relevant regulations, minimizing the potential for legal penalties.

Moreover, training prepares employees for incident response, fostering a culture of accountability and vigilance. It also keeps the workforce updated on evolving data protection practices and reinforces the importance of following established policies. Ultimately, a well-informed team is crucial for safeguarding an organization's data assets and ensuring a robust data governance framework.

In early FY25, we released basic Data Governance training to all staff and will continue to develop and assign more in-depth training for council members, leadership, and the necessary working group members.

Key Performance Indicators

KPIs are crucial for measuring the effectiveness of data governance, fostering accountability, driving continuous improvement, aligning with business objectives, enhancing communication, and managing risks effectively.

While we don't currently have formal data governance KPIs, we plan to develop and implement them during FY25, as we define our policies, create processes for incident management, and document Critical Data Elements (CDE) and related meta-data.

Initially, we are considering three possible key areas for measurement:

- Data Quality Score: % of critical data elements meeting quality standards.
- Incident Response Time: Average time to resolve data governance incidents.
- Compliance Rate: % of adherence to data governance policies.

More information will be shared on the Data Governance SharePoint site.

Data Governance Roadmap Maintenance

The **Technology Department** is responsible for administering, reviewing, and making recommendations for updates or changes to the Data Governance Roadmap in alignment with business needs.

This roadmap documentation will be reviewed annually by the Technology Department and Data Governance Council to ensure it remains current and relevant. Any updates or amendments to this document must be approved by the Council and communicated to all relevant stakeholders.

Contact Information

You may reach out to the Data Governance Council at DataGovernance@water.org. For more personal or confidential questions or information please contact the Director of Technology, kbridges@water.org.

Additional Resources

Related Policies and Documentation
- Data Governance Charter
- Data Governance SharePoint site
- Data Governance Definitions