Audit of Data Governance

Internal Audit Report
Prepared by: Audit and Assurance Services Branch

September 2023

Indigenous Services Canada
Services aux Autochtones Canada

Canada

Table of Contents

Acronyms

CDO	Chief Data Officer
CFRDO	Chief Finances, Results and Delivery Officer
CIO	Chief Information Officer
DAGC	Data and Analytics Governance Committee
DASRB	Data Access and Sharing Review Board
DGIOC	Directors General Implementation and Operations Committee
DAMA	Data Management Association
DMBOK	Data Management Body of Knowledge
DRF	Departmental Results Framework
DSN	Data Stewardship Network
GoC	Government of Canada
ISC	Indigenous Services Canada
ISO	International Organization for Standardization
KPI	Key Performance Indicator
KRI	Key Risk Indicator
OSDC	Operations and Services Delivery Committee
ROD	Record of Decision
SPP	Strategic Policy and Partnerships
TB	Treasury Board

Executive Summary

In 2019, Indigenous Services Canada (ISC) developed a Departmental Data strategy to help guide the achievement of departmental objectives. To oversee the effectiveness of the data strategy, an interim data governance function was implemented within ISC, supported by the existing Chief Information Officer position and a new Chief Data Officer position that was created in 2021.

The audit of Data Governance was included in ISC's Risk-Based Audit Plan for 2022-2023, which was presented to the Departmental Audit Committee and approved by the Deputy Minister in June 2022.

The audit objective was to provide assurance that ISC has a sound data governance function and structure with processes in place to support the management of departmental data.

The audit found various gaps in ISC's data governance, posing risks to the Department's ability to effectively utilize data and implement the *Data Strategy for the Federal Public Service*. Key issues identified include: an incomplete inventory of data holdings, no formalized processes for risk management, and gaps in the communication of roles and responsibilities. In addition, there is no systematic approach to tracking stakeholder feedback on data governance initiatives or to the monitoring of corrective actions.

ISC's data governance maturity level was assessed across all four data governance pillars and the Department's current maturity level is 'Initial' or 'Limited', indicating the need for continued improvement. As a result, the audit has identified the following recommendations:

1. **Objective alignment and formalized decision making, prioritization and monitoring** – The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in consultation with the Chief Finances, Results and Delivery Officer should ensure that existing data governance objectives are aligned with the departmental plan and core service areas. Formalized processes should be established for monitoring and tracking performance, prioritizing, and overseeing the portfolio of data governance workplan items. Additionally, these processes should include clear accountabilities and mechanisms for decision-making, prioritization, taking corrective actions, and capturing feedback from key stakeholders.
2. **Data stewardship roles and responsibilities** – The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in consultation with the Chief Finances, Results and Delivery Officer should establish a structured approach to data stewardship within the Department. This involves formally defining data stewardship roles and responsibilities to align with the data governance objectives and requirements of the Department. Simultaneously, an Executive Data Steward and Data Stewardship Network membership list should be completed and validated, with roles and responsibilities clearly documented and communicated. Additionally, a comprehensive onboarding and training program for data stewardship should be developed to ensure that individuals fully understand their responsibilities and contribute effectively to data governance.
3. **Formalized data planning process** – The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in consultation with the Chief Finances, Results and Delivery Officer

should align policy instruments to a data lifecycle approach and establish a formalized process that clearly defines roles and responsibilities for obtaining a complete view of the data in their inventory, as well as identifying data gaps and data needs.

4. **Data quality framework** – The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in consultation with the Chief Finances, Results and Delivery Officer should establish and implement a complete data quality framework to ensure that the departmental data meets the Treasury Board of Canada Secretariat requirements of accessibility, interoperability, and protection of privacy and confidentiality (Guideline on Service and Digital, Section 3).
5. **Enhance Data Security and Integrity** – The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in collaboration with the Chief Finances, Results and Delivery Officer should implement robust data loss prevention strategies and mechanisms to improve the security data. These mechanisms should prevent unauthorized data access and sharing both within and outside the Department. The implementation process should be clearly documented, communicated across the Department, and regularly reviewed for effectiveness and potential improvements.
6. **Data Governance Awareness** – The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in consultation with the Chief Finances, Results and Delivery Officer should implement a robust user communication strategy promoting data governance awareness among key stakeholders. This strategy should include highlighting the key elements of data governance framework, data policies and tools, data governance initiatives currently underway, and the importance/value of high-quality data and risks associated with poor data utilization. In addition, establish a feedback mechanism to track and act on feedback from employees related to data governance, aiding continuous improvement of data governance activities and practices.

Statement of conformance

The audit conforms with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* and the Government of Canada's *Policy on Internal Audit*, as supported by the results of the Quality Assurance and Improvement Program.

Management's response

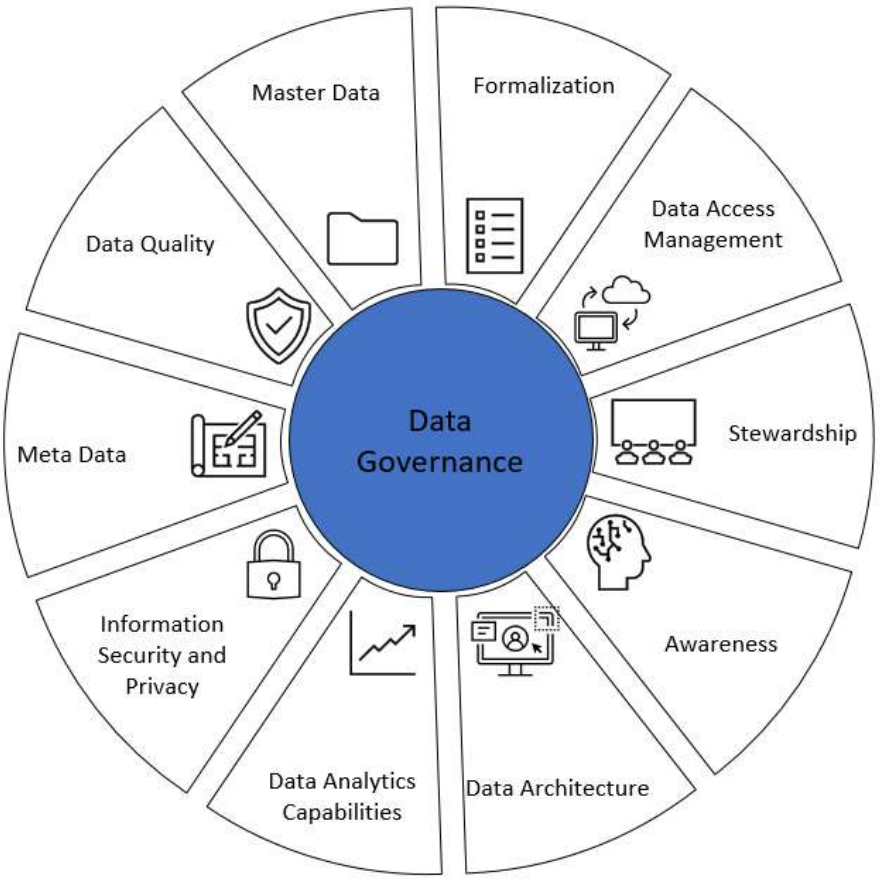
Management is in agreement with the findings, has accepted the recommendation included in the report and has developed a management action plan to address it. The management action plan has been integrated into this report.

1. Context

1.1 Data governance and its importance at ISC

Data governance is defined by the Data Management Association (DAMA) as the organizing framework for establishing the strategy, objectives, and policy for effectively managing corporate data. Data governance provides a framework for data management to engage and align with the business priorities and stakeholders and enables the effective use of data for timely decision making to support departmental programs. By referencing data governance industry best practice guidance (e.g., DAMA, Stanford, International Business Machines (IBM), etc.), an organization's data governance can be assessed across the following areas as depicted in Figure 1 below.

Figure 1: DAMA Data Governance Assessment Areas



ISC is responsible for providing a wide range of services and programs to Indigenous communities, including healthcare, education, social services, and infrastructure development. To achieve its departmental objectives, ISC relies heavily on data and effective data governance is essential to ISC achieving its short-term (i.e., deliver effective services) and long-term (i.e., transfer of services) goals. Data informs policy and program decisions, measures outcomes, and can improve service delivery for Indigenous communities in Canada. An example of one of the

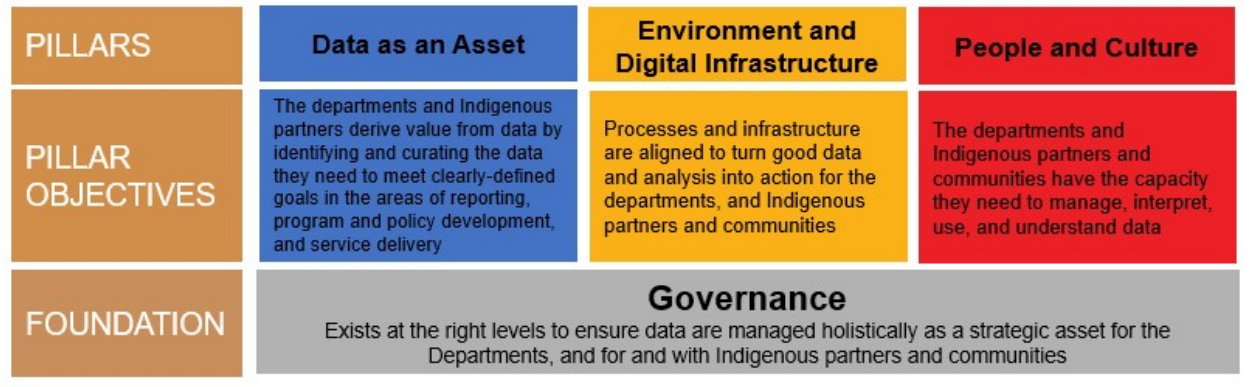
Department's most data-intensive processes is the administration of transfer payment funding. This process requires ISC to collect and review an extensive amount of data from a variety of programs and financial reports. This data informs contribution funding decisions for funding recipients including First Nations, Tribal Councils, and other Indigenous organizations. Another enterprise-wide data-intensive process within the Department is the measurement of Departmental results, where the Department leverages complex data to measure program and service performance through key performance indicators (KPIs) and key risk indicators (KRIs). These indicators are used to measure outcomes and ultimately inform strategic departmental decisions (e.g., Memoranda to Cabinet, Treasury Board submissions, etc.). As such, it is imperative that a strong data governance function exists within the Department to support and enable complete, accurate, timely and fit-for-use information in support of critical business decisions. Without an effective data governance function, there is a risk that key departmental stakeholders are making decisions based on data that is not complete, accurate and/or timely.

Furthermore, effective data governance functions with supporting data practices are necessary to achieve ISC's objective of transferring programs and services to Indigenous communities. In 2018, the importance of data governance and supporting data practices was highlighted in the Data Strategy Roadmap which was published by the Clerk of the Privy Council for the Government of Canada (GoC). This Roadmap included a specific recommendation to support Indigenous data strategies and co-develop distinctions-based strategies to help advance Indigenous data governance and co-develop indicators and data collection strategies.

1.2 ISC's Data Governance Function

The Data Strategy Roadmap for the GoC called on all federal departments to have their own data strategies in place by September 2019. Accordingly, in 2019, ISC developed a Departmental Data strategy to help guide the achievement of its objectives. At the time, a data governance structure had not yet been established and as such, an interim data governance function was implemented within ISC in 2021 to guide the execution of data governance workplan items in alignment with data strategy objectives. Figure 2 illustrates the three key pillars of the Departmental Data Strategy and demonstrates the underlying role of governance in supporting each of them.

Figure 2: Departmental Data Strategy Pillars & Objectives



By leveraging data and the supporting infrastructure to achieve its departmental objectives, ISC must adhere to the requirements as defined in the Treasury Board of Canada's *Policy on Service and Digital.* This Policy defines guidance and expectations for federal government departments to provide high-quality digital services to Canadians. As described in the *Guideline on Service and Digital*, information and data are strategic assets that play an increasingly central role in supporting departmental operations, decision-making, and the design and delivery of services. For information and data to be effectively leveraged for their intended purpose, they must first be well managed. This supports the expected outcomes of the *Policy on Service and Digital* that information is managed as a strategic asset, throughout its life cycle. The Policy emphasizes the importance of data governance and for ISC specifically, the *Policy* has been referenced in the Department's data strategy and its data governance structure.

Roles and responsibilities of the Chief Information Officer (CIO) and Chief Data Officer (CDO):

As detailed in Treasury Board of Canada Secretariat's *Guideline on Service and Digital* and in alignment with industry best practice for data governance, the CIO is responsible for managing information and building an enterprise-wide approach to Data Quality. The CDO is responsible for supporting data governance and departmental capacity. CDOs can leverage data to support the Department's objectives.

Within the context of ISC specifically, the CIO and CDO jointly oversee the data governance function. The CIO primarily manages the Department's data management practices, whereas the CDO is primarily responsible for aligning the Department's overall and longer-term vision of data sharing and service transfer as well as the curation of data assets. Additionally, the CDO is responsible for developing and implementing an overall vision for using data as a strategic asset within the department to support service delivery, transformation, and transfer; and for supporting Indigenous governments and organizations to develop the data capacity they need to deliver services to their Peoples.

As co-chairs of ISC's data governance function, the CIO and CDO are accountable for overseeing the achievement of several data governance objectives including but not limited to:

- Promoting data stewardship through the role of an executive data steward, ensuring data under their purview is managed as an enterprise asset;
- Making key decisions regarding enterprise data; and
- Developing, endorsing, and implementing the departmental data strategy, data policy, and other recommendations.

Roles and responsibilities of the Data Stewards:

Data stewards play a critical role in implementing a data governance function across an organization. Given ISC is a large organization with extensive service offerings across Canada, data stewards are tasked with ensuring that the data within their program and/or regions is accurate, reliable, and secure. Their work includes identifying the critical departmental data elements, defining the rules for how the data should be collected, stored, and used, and

monitoring the data to ensure that it follows the rules. Additionally, data stewards help ensure that the established rules and data practices are communicated and monitored within the Department.

The Department has commenced the implementation of the Data Steward Network (DSN) which is a key mechanism to promote departmental awareness of ISC's approach to data, discuss data sharing concerns, collaborate to establish best practices for data management, and define roles and responsibilities related to data governance. Additionally, the department is taking steps to formalize the role of the Executive Data Steward so the responsibility and accountability for the work the Data Stewards undertake is clear and can be coordinated at an enterprise level.

2. About the Audit

The audit of data governance was included in Indigenous Services Canada's Risk-Based Audit Plan for 2022-2023, which was presented to the Departmental Audit Committee and approved by the Deputy Minister in June 2022.

2.1 Why it is important

The audit was identified as a priority because a strong data governance function is important for overseeing and providing guidance to the Department to ensure that key stakeholders are informed by complete, accurate, timely and fit-for-use information in support of critical business planning, decisions and timely and effective actions.

2.2 Audit Objective

The audit objective was to provide assurance that the Department had a sound data governance function with data practices in place to support the management of departmental data.

2.3 Audit scope

The scope of this audit focused on the centralized roles of the CIO in ISC's Chief Finances, Results Delivery Officer (CFRDO) Sector and the CDO in ISC's Strategic Policy and Partnerships (SPP) Sector as well as the collaborative work of their teams as they support data management within ISC through sound data governance practices. The audit examined the implemented Data Governance processes and activities that have been operationalized as a result of the approved Departmental Data Strategy (2020) and the approved interim Data Governance structure (2021).

The audit examined the adequacy of the governance structure and processes by assessing whether a data governance function and structure including key roles, responsibilities, and accountabilities had been established and communicated; governance processes were in place to manage data throughout its lifecycle and ensured that data integrity was factored into the governance process in order to enhance the usability of the data for decision making; and finally, that oversight and monitoring activities were occurring in order to meet Data Governance-related objectives and ensuring that concerns were raised with Senior Management as appropriate.

To assess the effectiveness of governance mechanisms, applicable existing controls were measured against Data Governance standards as defined in the Data Management Body of Knowledge (DAMA-DMBOK), the Treasury Board *Policy on Service and Digital*, and Government of Canada Digital Standards.

2.4 Audit approach and methodology

The audit was conducted in accordance with the requirements of the Treasury Board *Policy on Internal Audit* and followed the International Standards for the Professional Practice of Internal Auditing. Additionally, the audit approach incorporated guidance from relevant data governance control frameworks and reference materials:

- Data Management Association (DAMA) – Data Management Body of Knowledge (DMBOK);
- Report to the Clerk of the Privy Council: A Data Strategy Roadmap for the Federal Public Service; and,
- Treasury Board *Policy on Service and Digital*.

The audit examined sufficient, relevant evidence and obtained sufficient information to provide a reasonable level of assurance in support of the audit conclusion. The audit criteria can be found in *Annex A*. The main audit techniques used included:

- Interviews with key stakeholders involved in data governance that included walkthroughs of data governance processes such as developing policies, engaging key stakeholders and overseeing data stewardship;
- Documentation review including; governance committee Terms of References (ToR), supporting policies and processes, governance committee records of decisions, tools and checklists used to fulfill monitoring responsibilities;
- Completion of file testing activities on Data and Analytics Governance Committee (DAGC) workplan items across DAGC and Director General Implementation and Operations Committee (DGIOC) Records of Decision to assess completeness of documentation and corrective actions taken;
- A questionnaire, which yielded responses from 22 out of the 44 individuals (50%); and
- A data governance maturity assessment.

Sampling Strategy

Testing was performed to assess completeness of documentation and corrective actions taken on work plan items. Based on the frequency of updates to the DAGC workplan inventory, a random sampling methodology was used to select approximately 10% of the workplan items within each Data Strategy Pillar. Given the frequency of development of the workplan items and the population size, the audit team randomly selected 5 out of the 43 workplan items to obtain audit observations. Also, interviews were conducted with data stewards to assess their awareness and understanding of roles and responsibilities.

3. Key Findings and Recommendations

As defined in the *Data Strategy Roadmap for the Government of Canada*, the suggested GoC data strategy for all federal departments aims to achieve several desired outcomes including improved services, better reporting on results, increased evidence-informed decision making, increased intra and inter-governmental collaboration, among others. To achieve these desired outcomes, departmental data strategies were suggested by the Privy Council Office to leverage the pillars listed below.

- **Governance:** data is managed holistically as a strategic asset, with the corresponding accountability, roles and responsibilities;
- **Data as an asset:** the government has the data it needs, which are fit for use, discoverable, and available;
- **Environment and digital infrastructure:** processes and infrastructure are aligned to turn good data and analysis into action; and
- **People and culture:** the government has the talent and capacity it needs to manage, interpret, use and understand data.

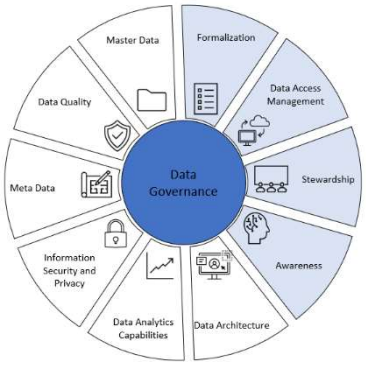
Summary of Findings

The audit identified several findings and opportunities for improvement to help ISC's data governance function achieve its strategic objectives and GoC priorities of supporting Indigenous data strategies. Key findings include gaps in the design, communication, and monitoring of the data governance policies, processes, and standards.

The audits findings are further explained in the following sections where each data strategy pillar includes the supporting details. Each data strategy pillar has been mapped to the corresponding assessment areas to demonstrate completeness, which references the assessment framework as outlined in Figure 1.

3.1 Governance

Background



Based on the *Guideline on Service and Digital*, the *Data Strategy Framework for the Federal Public Service,* and DAMA-DMBOK, and to help ensure that strategic objectives are being met, it was expected for the interim data governance structure Terms of Reference (ToR) objectives to be established and aligned to departmental strategic objectives as defined in ISC's 2021-2022 Departmental Plan and the 2021-2022 Departmental Results Framework (DRF). Additionally, it was expected that ISC's data governance leadership and committees would have clearly defined roles and responsibilities (e.g., DAGC, DSN), etc.). These are important to ensure that

there is clear responsibility and transparency for decision making and to ensure that decisions made align with the Department's strategic objectives.

To help facilitate the achievement of these objectives, it was also expected for the Department to have supplementary guidance materials and tools that facilitate the monitoring, oversight and prioritization of data governance workplan items (e.g., KPIs and KRIs).

If there isn't clearly defined roles and responsibilities for both data governance committees and data stewards, as well as no proper processes and tools in place, there may be a risk that data governance objectives may not be achieved. As such, decision-makers may not have the right direction, understanding of the data strategy, effective controls to ensure data integrity, and the support needed to ensure effective utilization of data for decision-making purposes.

Findings

Alignment of data governance objectives with departmental core service areas

Upon review, it was noted that the data governance objectives were not clearly aligned to strategic objectives as defined in the ISC 2021-2022 Departmental Plan and DRF core services areas (e.g., services and benefits to Individuals, health and social services, governance and community development services, Indigenous self-determined services). As part of the development of data governance objectives, a process to ensure completeness against objectives was not followed. More specifically, the interim data governance Terms of Reference (ToR) objectives did not include a rationale explaining how these objectives will facilitate the achievement of the planned results defined in the 2021-2022 Departmental Plan.

Alignment between data governance objectives and the strategic objectives is essential to ensuring the collection of relevant data and the effective management of that data. Misalignment may also lead to the data governance function's vision being incomplete and lacking an enterprise-view of ISC's strategic objectives.

Documentation of roles and responsibilities

Per DAMA guidance, defined and communicated management roles and responsibilities are essential for an effective data governance function. Otherwise, the function may lack a cohesive mechanism to guide the achievement of its objectives.

CIO and CDO

The CIO's and CDO's roles and responsibilities are documented, communicated, and understood.

Data Stewards

The roles and responsibilities of other key data governance roles beyond those of the CIO and CDO are not formalized. More specifically, it was noted that data stewards and related roles and responsibilities are not formally defined, communicated, and implemented. Without defined roles and responsibilities in the data governance space, there is not an authoritative source for

describing the expected responsibilities for collecting, using, storing and disposing of departmental data.

Data governance workplan

The data governance workplan tracker lists all data governance workplan items, as well as the associated deadlines, status, key contacts, and descriptions. While preliminary qualitative information existed to track performance (e.g., documented records of decision (RODs)), the audit team noted that there were no KPIs and KRIs in some of the workplans examined, which makes it difficult in effectively overseeing the broader data governance function. As a result, the Department may not be able to objectively measure and track historical performance of its data governance workplan items against departmental objectives. The lack of KPIs and KRIs also impacts the Department's ability to quantify its data needs and assess the data quality. Furthermore, it was noted that there was no prioritization mechanism in place for the various data governance workplan items examined. The auditees expressed that data governance KPIs and KRIs are to be developed as part of the implementation of the new DRF, which would inform the prioritization process.

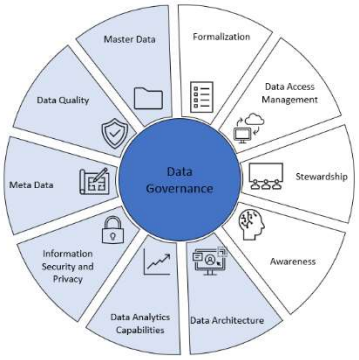
Recommendation(s)

1. **Objective alignment and formalized decision making, prioritization and monitoring** – The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in consultation with the Chief Finances, Results and Delivery Officer should ensure that existing data governance objectives are aligned with the departmental plan and core service areas. Formalized processes should be established for monitoring, prioritizing, and overseeing the portfolio of data governance workplan items. Additionally, these processes should include clear accountabilities and mechanisms for decision-making, prioritization, taking corrective actions, and capturing feedback from key stakeholders.

2. **Data stewardship roles and responsibilities** – The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in consultation with the Chief Finances, Results and Delivery Officer should establish a structured approach to data stewardship within the Department. This involves formally defining data stewardship roles and responsibilities to align with the data governance objectives and requirements of the Department. Simultaneously, an Executive Data Steward and Data Stewardship Network membership list should be completed and validated, with roles and responsibilities clearly documented and communicated. Additionally, a comprehensive onboarding and training program for data stewardship should be developed to ensure that individuals fully understand their responsibilities and contribute effectively to data governance.

3.2 Data as an Asset

Background



Identifying and treating data as an asset is essential to how an organization manages data, but it is also key to helping an organization become more information-centric with data as a core pillar of decision-making. Treating data as an asset is a key part of effective data governance.

Based on guidance provided by Treasury Board, the Privy Council's Office and DAMA, it was expected that the Department have a formalized process for identifying data needs, inventories, and gaps. Additionally, it was expected that the Department have a data quality framework in place that is aligned to a data lifecycle approach. This would help manage departmental data and key elements such as accessibility, interoperability, and protection of privacy and confidentiality. To enable informed decision-making, departmental stakeholders should have the data to meet their needs, which is fit for use, discoverable, and available. The audit team expected to see policies for data collection, and result reporting processes for relevant internal and external stakeholders, and a communication strategy for the data governance function and communicating data initiatives across the Department.

If there isn't any effective processes in place to ensure that data is fit for use and of high quality, there may be a risk that critical departmental data used in decision-making is not accurate, complete, or timely. This could result in poor decision-making related to informed policy and program decisions, improving service delivery, and measuring outcomes for Indigenous communities.

Finding

Departmental data planning (e.g., data needs, inventories, and gaps)

It was noted that there is no formalized process for obtaining a complete view of the data in inventory, as well as identifying data gaps and data needs. It was mentioned that this process and policy gap is largely driven by the fact that the existing policy instruments are outdated and are not based upon the lifecycle approach (see Annex B for more details related to the data lifecycle approach). Management has expressed that aligning the policy instruments to a lifecycle approach would allow the Department to identify and address the data gaps. Without a formalized process for identifying data needs, inventories and gaps, there is a risk that departmental stakeholders may lack the required data for decision-making.

The current approach to data planning is siloed, which is a result of the outdated policies. Limited data planning and utilization of a siloed approach to data needs identification may result in impacts to the relevancy of data, the ability of the data to improve decision-making as intended and gain insights on service provision, and the relationships with Indigenous partners. Effective data

planning helps streamline reporting requirements, reduce the reporting burden on Indigenous partners, and improve the decision-making process.

Data quality framework

Per the Guideline on Service and Digital and industry best practices outlined by DAMA and International Organization for Standardization (ISO)-8000 (as outlined in Annex C), a data quality framework is essential for managing key data elements such as accessibility, interoperability, and protection of privacy and confidentiality. Within the existing data governance policies, it was noted that there is not a complete departmental data quality framework (e.g., policies, procedures, and standards) in place for managing and overseeing the Department's data quality.

While the ISC Directive – Managing Information in a Digital Environment includes some key elements of data quality as required by the Treasury Board (TB) *Policy on Service and Digital*, several gaps were noted. These gaps include guidance on the storage of information, the protection of information against loss, and classification of data.

A complete and implemented data quality framework helps ensure that outputs are accurate, complete, reliable, interpretable, and data is accessed by authorized users. Any gaps in the framework may impact the quality and safety of the data and for Department like ISC that has significant data, it's essential to ensure its quality and safety.

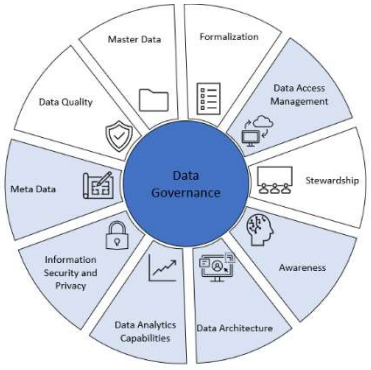
Recommendation(s)

3. **Formalized data planning process –** The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in consultation with the Chief Finances, Results and Delivery Officer should align policy instruments to a data lifecycle approach and establish a formalized process that clearly defines roles and responsibilities for obtaining a complete view of the data in their inventory, as well as identifying data gaps and data needs.

4. **Data quality framework –** The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in consultation with the Chief Finances, Results and Delivery Officer should establish and implement a complete data quality framework to ensure that the departmental data meets the Treasury Board of Canada Secretariat requirements of accessibility, interoperability, and protection of privacy and confidentiality (Guideline on Service and Digital, Section 3).

3.3 Data Infrastructure Development, Feedback Mechanisms and Data Protection

Background



Ensuring process are in place to solicit and incorporate feedback is essential to continued improvement, especially with respect to data practices and digital infrastructure. Based on the TB Data Strategy Framework for the Federal Public Service, as well as DAMA-DMBOK, it was expected that the Department have monitoring mechanisms in place to capture feedback from key stakeholders. This would support continual improvement of departmental data governance policies, processes, and enabling infrastructure to turn data analysis into action. The audit team expected to find mechanisms for effectively documenting and monitoring progress on data initiatives and implementing corrective action when necessary. This includes processes to track progress on various data initiatives, clearly defined accountabilities, established timelines, status updates on corrective actions, and detailed mechanisms for prioritizing data governance workplan items.

Moreover, it was anticipated that the Department would have control mechanisms in place to prevent sensitive data from leaving the Department, thereby enhancing data confidentiality, privacy, and security. These controls might include formal employee training, endpoint protection on devices, and remote wiping capabilities on Department-owned devices. The audit team also expected to find mechanisms for collecting employee feedback, such as feedback forms, surveys, and designated feedback channels.

If there isn't any formalized processes to document key decisions and monitor the progress of data governance workplan items, the Department may not have the required information to monitor the progress made and risks against its strategic objectives.

Additionally, if there are no controls to prevent data loss, there may be a risk that sensitive data could be shared with unauthorized users within or outside of the Department, resulting in potentially adverse reputational and operational impacts.

If there are no monitoring mechanisms in place to capture feedback from key stakeholders, there may be a risk that existing processes for receiving feedback as part of the oversight process are not adequate, resulting in implementation concerns not being raised with Senior Management and a lack of actionable insights to help improve departmental data strategies and data governance practices.

Findings

Data governance workplan monitoring

It was noted that the Department has implemented a workplan tracker as the key mechanism for monitoring the progress of various data governance workplan items. However, there was not a formalized process in place to document and monitor performance, decisions, risks, and corrective actions. Through testing of the sampled workplan items, it was noted that there were not consistently defined accountabilities, timelines and corrective actions. Additionally, it was noted that one of the sampled workplan items was cancelled without a documented decision or rationale within the reviewed RODs. Although there were follow-up inquiries, the audit team did not receive evidence to clarify why this decision was made.

Clearly defined and communicated accountabilities, timelines, and a formalized decision-making process where decisions are documented and essential to ensuring the effective implementation of current and future data governance workplan items. Processes are required to ensure that workplan item performance and risk trends are being monitored and corrective actions are taken where applicable.

Feedback mechanisms

The Department does not have formal processes (e.g., a central repository) to holistically track departmental data governance feedback. Examples of expected feedback elements include the performance of key departmental data sets and source systems, performance of data governance workplan items, and insights provided by key stakeholders. It was noted that the Department has modular feedback tracking mechanisms in place, but there is no centralized tracking across the broader data governance function. The audit found that feedback is primarily addressed through email communications, directly with clients, or at times through regularly conducted governance meetings (e.g., DGIOC and Operations and Services Delivery Committee (OSDC)).

Without processes and mechanisms to log and track feedback horizontally, there is a risk that issues are not identified and addressed promptly. There is a risk that management may miss out on valuable perspectives, which could ultimately negatively affect the data governance and management process and decision-making, which may impact services to Indigenous communities.

Data loss prevention mechanisms

The audit found that there were formalized tools and processes in place for managing external data-sharing. More specifically, the Department has implemented a data access and sharing review board (DASRB), which aims to mitigate risks concerning external data access and sharing. However, at an enterprise level, there is not a formal process for data loss prevention. Management acknowledged that there are no data loss prevention tools or processes to prevent unauthorized data from leaving the Department. For example, sensitive data can be transferred to a USB stick and sent to someone as there are currently no detection mechanisms to prevent or flag the data loss. It was noted that the same risk is present while using desktops, laptops, and external hard drives. Without a formalized data loss prevention mechanism, there is a risk that sensitive data could be shared with unauthorized users within or outside of the Department. This is also a significant reputational risk as the Department is in possession of sensitive data.

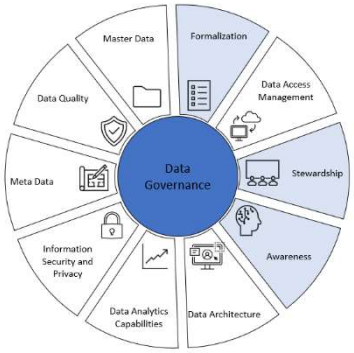
Recommendations

Please refer to **recommendation #1** in **section 3.1** for the recommendation related to monitoring mechanisms.

5. **Enhance Data Security and Integrity** – The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in collaboration with the Chief Finances, Results and Delivery Officer should implement robust data loss prevention strategies and mechanisms to improve the security data. These mechanisms should prevent unauthorized data access and sharing both within and outside the Department. The implementation process should be clearly documented, communicated across the Department, and regularly reviewed for effectiveness and potential improvements.

3.4 People and Culture

Background



The culture of an organization plays a pivotal role in effective data governance. A data-driven culture fosters understanding, acceptance, and consistency in managing data's availability, relevancy, usability, integrity, and security. In an environment where data is truly valued (i.e., an asset), stakeholders are more likely to adopt robust governance strategies, ensuring the data's consistent and optimal use. A key element of fostering this culture is ensuring effective communication and awareness of responsibilities and the value/benefits of effective data governance.

Based on guidance provided by Treasury Board, the Data Strategy Framework for the Federal Public Service, as well as DAMA-DMBOK, it was expected that the Department have a user communication strategy for promoting awareness among key stakeholders. It was expected that the communication strategy includes details of the data governance function's desired outcomes, with the goal of increasing participation and adoption of data governance initiatives. More specifically, it was expected that a documented terms of reference be in place for the data stewards where the following are defined: roles and responsibilities, organizational charts with a complete membership for ISC's regional and program data stewards, and training and onboarding for new data stewards. Overall, data governance policies, processes, and standards were expected to be communicated to ensure that key stakeholders are informed of how to manage, interpret, use and understand data.

If there is no user communication strategy in place to engage key stakeholders, there may be a risk that key stakeholders are unaware of data governance strategy, policies, processes, and standards, resulting in strategic objectives not being met. This could limit the implementation of such policies and process, and result in non-compliance with established guidelines as well as limiting the implementation of the culture needed for effective data governance. Additionally, if there isn't complete representation of data stewards within the DSN, there may be a risk that

certain data steward responsibilities are not being performed and that inefficiencies could arise such as delays in performing data steward activities. In turn, the timelines and quality of data-driven activities may be affected.

Findings

Completeness of data stewardship network membership

It was noted that the DSN membership list was incomplete since there were vacant data stewards within the DSN for certain program and regional areas. It was also noted by management that the DSN membership list has yet to be validated with its detailed data stewards. Identification of key personnel responsible for data stewardship is an essential primary step to ensuring implementation of effective data governance.

Communication and awareness of data steward roles and responsibilities

Once the data stewards have been identified, it is important to communicate their roles and responsibilities to them and the supporting personnel tasked with executing data steward objectives. The audit found that roles and responsibilities for data stewards were not formally documented or communicated. Currently, data stewards discuss data issues and are informed of their roles and responsibilities on an ad-hoc basis with the data governance function through DGIOC and OSDC meetings. At the time of the audit, it was noted that some training initiatives aimed at providing data stewards with information specific to their role were cancelled.

Furthermore, the audit team sent a questionnaire to all data stewards and found that the majority of the respondents indicated that they were generally aware of a data governance function and the roles and responsibilities of the function within the Department as well as the associated committees. However, some data stewards were generally uncertain of their role within the data governance function and were unsure how DSN fit into the broader data governance function and supported their role.

Without formalized processes and defined roles and responsibilities, there was a lack of evidence to enable the Department to conclude whether the DSN is achieving its intended outcomes, including promoting departmental awareness of ISC's approach to data, discussing data strategies, and collaborating to establish best practices for data management among others.

A clear data governance strategy with associated roles and responsibilities of the key stakeholders, like data stewards, that is well communicated and monitored through existing committees is essential to ensuring the continued maturity of ISC's data governance.

Recommendation(s)

Please refer to **recommendation #2** in **section 3.1** for the recommendation related to stakeholder identification.

6. **Data Governance Awareness** – The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in consultation with the Chief Finances, Results and Delivery Officer

should implement a robust user communication strategy promoting data governance awareness among key stakeholders. This strategy should include highlighting the key elements of data governance framework, data policies and tools, data governance initiatives currently underway, and the importance/value of high-quality data and risks associated with poor data utilization. In addition, establish a feedback mechanism to track and act on feedback from employees related to data governance, aiding continuous improvement of data governance activities and practices.

3.5 ISC Data Governance Maturity

The audit examined key elements of the ISC data governance framework. Additionally, the team performed an assessment of the data governance maturity level using the Stanford Data Governance Maturity Model and drew upon data governance best practices from the Data Management Body of Knowledge. This assessment was used to gauge the Department's maturity level on a scale from 1 to 5. On this scale, 1 signifies an "Initial" maturity level and 5 represents the "Best" level, according to the model.

The model assesses two primary categories: foundational and projects. Under the foundational category, the following elements were included and assessed:

- **Formalization:** The extent to which roles are structured in an organization and the activities of the employees are governed by rules and procedures.
- **Awareness:** The extent to which individuals within the organization are aware of the roles, rules, and technologies associated with the data governance program or function.
- **Metadata:** Data that describes other data and IT assets, such as databases, tables, and applications, by relating essential business and technical information. It facilitates consistent understanding of the characteristics and usage of data.

The project category includes:

- **Stewardship:** The formalization of accountability for the definition, usage, and quality standards of specific data assets within a defined organizational scope.
- **Data Quality:** The continuous process for defining the parameters for specifying acceptable levels of data quality to meet business needs, and for ensuring that data quality meets these levels.
- **Master Data:** The core data essential for operations. What is considered master data can vary depending on the organization.

The assessment process entailed a review of available documentation, including data governance policies and processes, conducting walkthroughs and interviews with key stakeholders. The result of the assessment identified ISC’s data governance maturity at a level 1 to 2 out of 5, meaning data governance is “Initial” to “Limited”. These results reflect the relatively recent development of an ISC data strategy in 2019 and the creation of a key position, the Chief Data Officer, in 2021.

4. Conclusion

When ISC developed its Departmental Data Strategy in 2019, an existing data governance structure had not yet been established. Since then, the Department created the role of the CDO and an interim data governance function to guide the execution of data governance workplan items. While some steps were taken to advance data governance throughout the Department, the audit found gaps in the current data governance function. More specifically, an effective data governance function requires a robust framework that addresses all facets of data governance, with collaboration from sectors and regions. To shift the Department towards a data-driven model, the Department requires decisions that are informed by relevant and secure data, awareness of the strategy, identification of key stakeholders, and oversight of the implementation process. This should include solicitation of feedback to ensure continuous improvement of both the process and strategy.

The audit findings indicate that there are several gaps in data governance, and recommendations have been provided to enhance the Department's data governance functions. These enhancements pertain to the design, communication, and monitoring of data governance policies, processes, and standards. The maturity assessment ranks the Department's data governance maturity as 'Initial' or 'Limited' (levels 1 or 2) across the key data governance pillars. If these gaps are not adequately managed, the Department may find it difficult to meet its current strategic objectives and the broader data priorities set for 2023-2026 by the GoC.

While the 2018 Data Strategy Roadmap was the Government of Canada's (GoC's) data strategy framework for the audit scope's temporal period, an updated version was released in 2023 – the 2023–2026 Data Strategy for the Federal Public Service. The updated GoC data strategy introduces a new data strategy framework and pillars. However, the desired outcomes remain largely similar to the 2018 Data Strategy Roadmap (e.g., supporting Indigenous data sovereignty, enhancing evidence-informed decision-making, improving services, etc.).

5. Management Action Plan

Recommendations	Management Response / Actions	Responsible Manager (Title)	Planned Implementation Date
1. **Objective alignment and formalized decision making, prioritization and monitoring** – The Assistant Deputy Minister (ADM) of the Strategic Policy and Partnerships (SPP) Sector in consultation with the Chief Finances, Results and Delivery Officer (CFRDO) should ensure that existing data governance objectives are aligned with the departmental plan and core service areas. Formalized processes should be established for monitoring and tracking performance, prioritizing, and overseeing the portfolio of data governance workplan items. Additionally, these processes should include clear accountabilities and mechanisms for decision-making, prioritization, taking corrective actions, and capturing feedback from key stakeholders.	The Chief Data Officer (CDO) and Chief Information Officer (CIO) will engage with and seek active cooperation from all sectors to develop an updated Departmental Data Strategy, ensuring that data governance objectives are aligned with the departmental plan and core service areas.	Chief Data Officer, Strategic Research and Data Innovation Branch, SPP Chief Information Officer, Information Management Branch, CFRDO	Q2, 2023-24
	The Chief Data Officer and Chief Information Officer will engage with and seek active cooperation from all sectors to: 1) Update and refine the current processes in place to monitor and track performance on the Data Strategy work plan items. This will include exploration and implementation, where appropriate and feasible, of digital tools to support monitoring and associated reporting processes. 2) Strengthen existing prioritization processes for current and future Data Strategy work plan items, include clear accountabilities and mechanisms for decision-making, taking corrective actions, and capturing feedback from stakeholders.	Chief Data Officer, Strategic Research and Data Innovation Branch, SPP Chief Information Officer, Information Management Branch, CFRDO	Q1, 2024-25

	A methodology will be developed in consultation with sectors to ensure objective and robust prioritization of work plan items based on alignment with federal and departmental priorities; but also incorporating considerations such level of effort, level of complexity, and impact; as well as the availability of human and financial resources to complete the work. This methodology will be annexed to an updated Terms of Reference for the Data and Analytics Governance Committee (DAGC).		
2. **Data stewardship roles and responsibilities** – The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in consultation with the Chief Finances, Results and Delivery Officer should establish a structured approach to data stewardship within the Department. This involves formally defining data stewardship roles and responsibilities to align with the data governance objectives and requirements of the Department. Simultaneously, an Executive Data Steward and Data Stewardship Network membership list should be completed and validated, with roles and responsibilities clearly documented and communicated. Additionally, a comprehensive onboarding and training program for data stewardship should be developed to	The Chief Data Officer and Chief Information Officer will engage with and seek active cooperation from all sectors to establish a structured approach to data stewardship within the Department. This will include a formal refresh of the data governance structure that will be submitted to senior management for approval and that will include: • Updated Terms of Reference for the Data and Analytics Governance Committee (DAGC). • Formalized roles and responsibilities defining Executive Data Steward, Data Steward, and Data Custodian, to complement the existing roles of the Chief Data Officer and Chief Information Officer. • A list of positions associated with these roles for different data assets, and a requirement that Executive Data Stewards support the Chief Information Officer in keeping this list up to date as part of the Data Asset Inventory.	Chief Data Officer, Strategic Research and Data Innovation Branch, SPP Chief Information Officer, Information Management Branch, CFRDO	Q1, 2024-25

ensure that individuals fully understand their responsibilities and contribute effectively to data governance.	• Formal Terms of Reference for the Data Stewardship Network including membership list.		
	The Chief Data Officer and Chief Information Officer will work towards establishing a comprehensive onboarding and training program for data stewardship. Planned work will focus on: - Developing and maintaining a curated list of data and data stewardship training courses and making it available in a Data Knowledge Centre in the Enterprise Performance and Information Centre (EPIC). - Delivering training sessions related to external data sharing. -Continued curation of presentations/information sharing on best practices in data stewardship, delivered through the Data Stewardship Network.	Chief Data Officer, Strategic Research and Data Innovation Branch, SPP Chief Information Officer, Information Management Branch, CFRDO	Q3, 2023-24
3. Formalized data planning process – The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in consultation with the Chief Finances, Results and Delivery Officer should align policy instruments to a data lifecycle approach and establish a formalized process that clearly defines roles and responsibilities for obtaining a	The Chief Data Officer and Chief Information Officer will align policy instruments to a data lifecycle approach and establish a formalized process that clearly defines roles and responsibilities for obtaining a complete view of the data in their inventory, as well as identifying data gaps and data needs.	Chief Data Officer, Strategic Research and Data Innovation Branch, SPP Chief Information Officer, Information Management Branch, CFRDO	Q4, 2023-24
	This work will produce:		Q4, 2023-24

complete view of the data in their inventory, as well as identifying data gaps and data needs.	• An assessment of data planning strengths and gaps in Treasury Board Submissions (in consultation with CFRDO).		
	• An assessment of the quality of select indicators and associated data in program Performance Information Profiles (PIPs) (in collaboration with Departmental Planning and Management Practices (DPMP)).		Q3, 2023-24
	• A departmental Data Asset Inventory as a tool to support Executive Data Stewards to effectively govern and manage the data under their care and control, and provide an enterprise view of the data assets in place across the department (in collaboration with all sectors).		Q3, 2023-24
4. Data quality framework – The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in consultation with the Chief Finances, Results and Delivery Officer should establish and implement a complete data quality framework to ensure that the departmental data meets the Treasury Board of Canada Secretariat requirements of accessibility, interoperability, and protection of privacy and	The Chief Data Officer and Chief Information Officer will establish and implement a data quality framework that reflects Treasury Board Secretariat's existing *Guideline on Service and Digital* (Section 3), but also the *Guidance on Data Quality* that is currently being developed by Treasury Board Secretariat. ISC's Data Quality Framework will be designed to support the assessment of PIP indicators as described above.	Chief Data Officer, Strategic Research and Data Innovation Branch, SPP Chief Information Officer, Information Management Branch, CFRDO	Q3, 2023-24
	In addition, the Chief Data Officer and Chief Information Officer will advance best practices in data development and management through: • participation in the development of Treasury Board Secretariat's implementation of the		Ongoing starting Q2, 2023-24

confidentiality (Guideline on Service and Digital, Section 3).	2023-2026 Data Strategy for the Federal Public Service;		
	• prioritizing and implementing key projects to strengthen the department's alignment with emergent federal standards. Initiatives include: • increased centralization of data in ISC's Enterprise Data Hub targeting three new data sets this fiscal. Ongoing work will continue in subsequent years to incorporate more of the departmental data holdings for analytical purposes.		Q4, 2023-24
	• development of a Master List of Communities and publication on EPIC		Q3, 2023-24
	• development of an analysis/ feasibility study on the implementation of departmental interoperability standards to support reclaiming Indigenous names (in response to Truth and Reconciliation Commission Call to Action 17)		Q1, 2023-24
	• identification or establishment of a working group with Treasury Board Secretariat and other key stakeholders to advance the work on this Call to Action.		To be determined in collaboration with Treasury Board Secretariat
5. Enhance Data Security and Integrity – The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in collaboration	The Chief Data Officer and Chief Information Officer will engage with and seek active cooperation from all sectors to implement robust	Chief Data Officer, Strategic Research and	Q3, 2023-24

with the Chief Finances, Results and Delivery Officer should implement robust data loss prevention strategies and mechanisms to improve the security data. These mechanisms should prevent unauthorized data access and sharing both within and outside the Department. The implementation process should be clearly documented, communicated across the Department, and regularly reviewed for effectiveness and potential improvements.	data loss prevention strategies and mechanisms to improve the security of data. They will: • Finalize and implement a Guide to External Data Sharing, which will clarify roles, requirements, and processes surrounding data sharing, including key privacy and security considerations.	Data Innovation Branch, SPP Chief Information Officer, Information Management Branch, CFRDO	
	• Develop a Policy on External Data Sharing which may necessitate changes to those roles, requirements, and processes, which would be reflected in subsequent versions of the Guide.		Q4, 2025-26
	• Develop a communications approach and training to support the implementation of the Guide.		Q3, 2023-24
	• Include in the Data Asset Inventory security parameters prescribed by Executive Data Stewards.		Q3, 2023-24
	• Provide and facilitate governance of the infrastructure (i.e., the Enterprise Data Hub) required for program areas to increasingly curate ISC data for decision making in a secure environment, and to publish to EPIC where data sensitivity permits, further advancing an “Open by Default” approach. Note: Additional capacity under the CIO required to perform the work as current team is at full capacity addressing operational requirements.		Q4, 2023-24

	• Strengthen mechanisms to monitor data leaving the department, including an Information Sharing Agreement inventory, a formal mandate for Executive Data Stewards to log all sharing of data that is under their care and control, and the development of a reporting tool and metrics to support the oversight role of the Chief Data Officer and Chief Information Officer.		Q1, 2024-25
6. Data Governance Awareness – The Assistant Deputy Minister of the Strategic Policy and Partnerships Sector in consultation with the Chief Finances, Results and Delivery Officer should implement a robust user communication strategy promoting data governance awareness among key stakeholders. This strategy should include highlighting the key elements of data governance framework, data policies and tools, data governance initiatives currently underway, and the importance/value of high-quality data and risks associated with poor data utilization. In addition, establish a feedback mechanism to track and act on feedback from employees related to data governance, aiding continuous improvement of data governance activities and practices.	The Chief Data Officer and Chief Information Officer, in collaboration with Communications Sector, will develop a robust communication strategy promoting data governance awareness among key stakeholders. It will include mechanisms to collect and/or consolidate feedback.	Chief Data Officer, Strategic Research and Data Innovation Branch, SPP Chief Information Officer, Information Management Branch, CFRDO	Q3, 2023-24
	Implementation of this communication strategy will roll out in an ongoing way. It will focus on leveraging EPIC as a digital single window for ISC employees to access departmental authoritative data holdings, analytics, business intelligence tools, and policies and guidance related to data; as well as the Data Stewardship Network and other relevant fora (e.g., Network for Sharing Indigenous Information and Research) and tools (e.g. the Express).		Ongoing, starting Q3, 2023-24

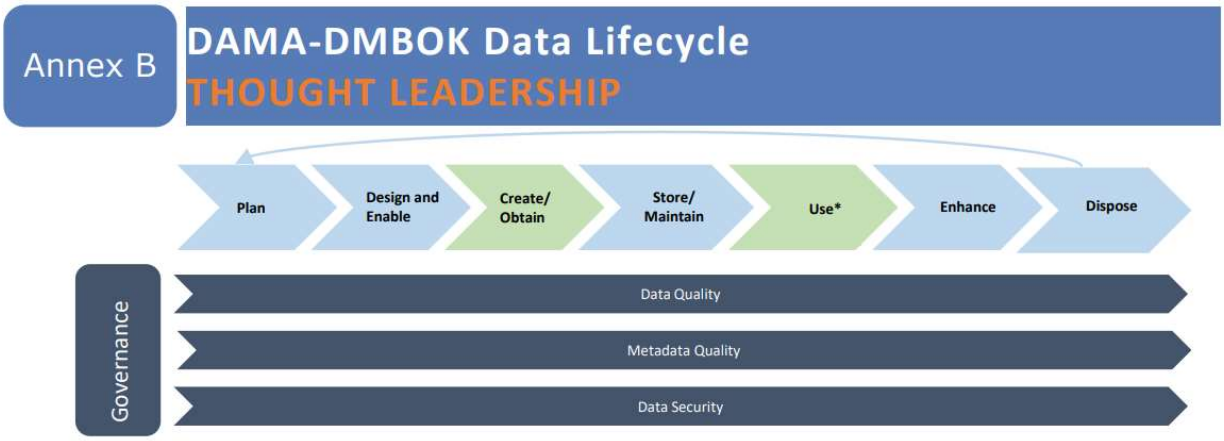
Annex A: Audit Criteria

To ensure an appropriate level of assurance to meet the audit objectives, the following audit criteria were developed to address the objectives.

Audit Criteria	Sub-criteria
1. ISC has implemented an effective data governance function and structure that guides and directs the management of data in the Department.	1.1 A clear data governance function and structure has been established and roles and responsibilities have been defined and communicated. 1.2 Data governance objectives have been established and are aligned with departmental strategic objectives. 1.3 Data governance bodies are actively participating in the development of departmental data management policies and the identification of procedures and supporting infrastructure needed to effectively utilize data. 1.4 Departmental data policies are up-to-date, comply with the relevant Government of Canada polices and incorporate key elements of data integrity.
2. An oversight process is in place to ensure the implementation of the Department's data strategy, objectives, and policies.	2.1 Data governance implementation plan exists with mechanisms to monitor progress made towards data initiatives and take corrective actions where necessary 2.2 Feedback received as part of the oversight process is used to improve departmental data strategies and implementation concerns are raised with Senior Management.

Annex B: DAMA-DMBOK Data Lifecycle Diagram

The presented diagram serves as an informative tool, aimed at facilitating readers' comprehension of the DAMA-DMBOK data lifecycle concept and its application within the context of ISC. The visual representation illustrates the essential data governance domains associated with each stage of the data lifecycle.



- **Governance:** Governance activities and oversight must be performed on all data lifecycle key activities to ensure that data quality, metadata quality, and data security are all managed in alignment with the organization's strategic objectives.
- **Data Quality**: Data quality must be considered throughout the data lifecycle, because data quality can be impacted by a variety of lifecycle events.
- **Metadata Quality**: Metadata must be managed in the same way as the quality of data, and must therefore be managed throughout the data lifecycle.
- **Data Security**: Data requiring protection must be protected throughout its lifecycle, from creation to disposal.

*Per DAMA-DMBOK's guidance, data creation/collection and data use are the most critical points in the data lifecycle. Data governance must be implemented with an understanding of how is produced, or obtained, and how data is used.

The data lifecycle of data at Indigenous Services Canada (ISC) can be broken down into several stages:

1. **Plan**: defining for data content requirements and data management requirements. These include program and service performance management indicators, corporate services, etc.

2. **Design and Enable**: Data content and data management requirements are defined in policy frameworks that define expectations for use, quality, controls, security and enterprise approach to architecture and design.

3. **Create/Collect:** Data is collected from various sources, including Indigenous communities, surveys, and administrative systems. ISC ensures that data is collected in a way that respects Indigenous values and principles, including privacy, confidentiality, and consent.

4. **Store/Maintain**: Data is stored securely in databases and other information systems. ISC ensures that data is stored in a way that protects the privacy and confidentiality of Indigenous Peoples and that it is accessible only to those who have a legitimate need for it.

5. **Use:** Data is shared with stakeholders, including Indigenous communities, government departments, and the public. ISC ensures that data is disseminated in a way that respects privacy and confidentiality and that it is presented in a way that is accurate, clear, and relevant to the needs of the intended audience.

6. **Enhance:** Data is processed to generate insights and support decision-making. This involves cleaning and validating the data, analyzing it to identify patterns and trends, and presenting the results in a way that is understandable and actionable.

7. **Dispose:** Data is archived or deleted at the end of its useful life. ISC ensures that data is archived in a way that preserves its integrity and that it is deleted in a way that complies with privacy and data protection laws and regulations.

Annex C: ISO-8000 Data Quality Framework

ISO 8000 stands as the internationally recognized standard for Data Quality and Enterprise Master Data, offering comprehensive direction on critical data quality aspects, such as portability, master data, reference data, and data maturity, among others. Given its significance, this framework has been incorporated herein for informational purposes, serving as a valuable reference to inform the development of a robust data quality framework.