Environment and Climate Change Canada | Environnement et Changement climatique Canada

Canada

Audit of information technology governance

AEB Audit and Evaluation Branch

DGAÉ Direction générale de l'audit et de l'évaluation

Cat. No.: En4-775/2025E-PDF
ISBN: 978-0-660-78426-7
EC: 25019.04

Environment and Climate Change Canada
Public Information Centre
Place Vincent Massey building
351 St-Joseph boulevard
Gatineau Quebec K1A 0H3
Toll free: 1-800-668-6767
Email: enviroinfo@ec.gc.ca

Aussi disponible en français

Table of Contents

1. Introduction

Objective

To assess the extent to which Environment and Climate Change Canada (ECCC) has an effective information technology (IT) governance structure in place that clearly identifies accountabilities and supports decision-making.

Context

Effective IT governance is critical to ensuring that technology, services, and information management support departmental objectives and align with Government of Canada priorities. In today's environment, IT governance functions within a broader digital context - one that includes oversight of service design and delivery, data, and cybersecurity - requiring departments to adopt more integrated and collaborative governance approaches.

The Treasury Board Canada's (TB) Policy on Service and Digital and its associated Directive, in effect since 2020, set expectations for this integrated approach. Departments must designate officials for key digital functions - including a Chief Information Officer (CIO), Designated Official for Service Management, Chief Data Officer, and a Designated Official for Cyber Security - and establish governance structures that align IT and digital investments with departmental priorities and government-wide direction. Deputy heads have the flexibility to assign these responsibilities at the level they deem appropriate, including assigning responsibility for more than one functional area to a single official.

Shared Services Canada (SSC) also plays a central role in this environment by providing mandatory government-wide infrastructure services - such as networks, data centres, and end-user technologies - which departments like ECCC rely on.

Program and service delivery officials are expected to work collaboratively with the CIO and other digital leads to ensure that digital solutions are integrated into business and operational planning and support client outcomes. Governance responsibilities extend to senior management committees, which oversee IT planning, investment prioritization, risk management, and performance monitoring. To support implementation and operational oversight, departments may establish supporting structures such as change advisory boards, architectural review panels, or project steering committees, where appropriate.

As a science-based department, ECCC depends on a wide range of internal systems, scientific applications, and external platforms such as the High-Performance Computing (HPC) to

support its mandate and mission-critical operations. Its digital governance environment has continued to evolve alongside organizational restructuring and expanding service delivery needs.

The audit period coincided with a time of significant structural transition in ECCC's digital governance - marked by the creation and reorganization of DSB, a broader departmental governance review, a DSB led digital governance review, and ongoing updates to IM/IT governance at the program level. These significant changes were brought in to address some of the longstanding IT governance issues that needed to be addressed and to support the department in its digital transformation journey – to enable a strong data and digital enabled workforce and to prepare for the emergence of artificial intelligence.

Scope and methodology

The audit focused on selected aspects of IT governance, including governance structures and oversight mechanisms that support accountability, strategic direction and decision-making, roles and responsibilities, as well as the mechanisms in place to manage the Department's relationship with SSC and related service delivery risks. The audit covered the period from April 1, 2023, to March 31, 2025, and included a review of other relevant documents outside this timeframe, where appropriate.

In-depth assessments of specific operational processes (such as project management, enterprise architecture, business continuity management, data and information management, IT asset management, etc.) were excluded from the scope due to their scale and complexity. While some of these areas were examined at a high level through the lens of governance, they may be considered in more detail through future internal audits as part of the annual risk-based audit planning process.

The audit criteria provided in Appendix A were developed based on the results of a risk assessment conducted during the planning phase of the audit.

The audit was conducted and completed using the following methods:

- Review of applicable policy instruments and over 550 documents, including governance and planning materials, and analysis of records from 18 IT-related committees and working groups.
- 29 interviews and walkthroughs with key personnel, and a questionnaire administered to 8 branches and 2 regions regarding input on their IT planning and prioritization processes.

- Review of 7 Service Agreements with SSC across 4 branches and a case study analysis of 2 mission-critical operations reliant on SSC-provided services.

Statement of conformance

The audit conforms to the Global Internal Audit Standards, as supported by the results of the quality assurance and improvement program.

2. Findings, recommendations, and management responses

2.1. Governance and roles and responsibilities

Key findings: ECCC's governance framework for digital and IT activities was in transition at the time of this audit. While progress has been made, such as the creation of the Digital Services Branch (DSB) and updates to senior-level governance committees – more work is needed to strengthen governance structures to support decision-making. This includes continuing work on clarifying roles, responsibilities, and accountabilities for digital and IT oversight to ensure that they are consistently defined, and departmental committees are effectively carrying out their roles in support of decision-making.

The areas identified for improvement include addressing outdated or incomplete terms of reference, strengthening linkages between committees, and parallel governance processes operating at the branch level. Opportunities also exist to clarify accountabilities, governance tools, and strengthen coordination across the Department in line with the Policy on Service and Digital.

What we examined

We assessed the extent to which ECCC had established an appropriate governance structure and framework to enable effective decision-making and support oversight and accountability for IT-related activities and associated risks. We also examined whether roles and responsibilities for IT governance were clearly defined, communicated, and understood, in alignment with policy requirements.

What we found

As set out in the Policy on Service and Digital and its supporting Directive and guideline, departmental CIOs are responsible for leading the departmental IT, information, and data management functions. This includes providing strategic leadership on digital and IT, overseeing departmental digital and IT planning, supporting integrated planning and governance across service, information, data, IT, and cyber security, overseeing information and data management practices, and leading enterprise architecture to ensure interoperability and alignment with enterprise standards.

Designated officials for service management and cyber security are likewise responsible for leading their respective functional areas. The designated official for service management promotes a departmental approach to service design and delivery, including coordinating service planning, performance measurement, service standards, and client feedback. The designated official for cyber security provides strategic leadership and coordination for cyber security, including risk-based protection of IT services, collaboration with the CIO and Chief Security Officer, and coordination of incident response and mitigation.

ECCC has made progress in aligning these leadership roles with government-wide digital policy, supporting clearer accountability to their respective functional areas. At ECCC, all three roles are situated within DSB. The ADM of DSB and Chief Service and Digital Officer, holds both the Departmental CIO and the designated official for service management roles. The designated official for cyber security is a Director General within the same branch.

IT governance bodies

To fulfill their responsibilities and support accountability, CIO and designated officials are expected to support and participate in integrated governance structures that enable oversight, coordination, and decision-making across digital functions. The Directive on Service and Digital emphasizes strategic leadership and cross-functional collaboration, while the Policy requires deputy heads to establish governance that integrates service, information, data, IT, and cyber security. Within this framework, committees serve as the primary mechanisms through which functional leads - such as the CIO and the designated officials - exercise their responsibilities, provide advice, and help align digital initiatives with departmental and enterprise priorities.

At ECCC, IT governance landscape includes a mix of internal and external structures. Internally, the Department has committees and forums at the corporate, enterprise (led by DSB), and program or branch levels. Externally, ECCC participates in interdepartmental and government-wide bodies that influence or support ECCC IT-related activities. The following

overview reflects the structures identified during the audit but may not include the complete list of all existing or emerging governance bodies.

The committees and groups vary in mandate and are at different stages of alignment with either legacy or emerging governance models. At the enterprise-level, governance is supported by DSB, which chairs or coordinates several committees or advisory bodies, with functional direction provided by the Chief Service and Digital Officer, who oversees digital service management and departmental alignment with federal priorities, including the Architecture Change Management Board, the Architecture Review Group, the Digital Modernization Steering Committee, the Data Policy and Priorities Committee, and the DSB Digital Transformation Committee. These are intended to support enterprise architecture oversight, strategic digital planning, and alignment with federal digital policy.

Other areas of management – such as project management, security, financial management and investment planning – also have implications for IT, digital, and service functions. These areas are supported or overseen by corporate level committees. Some of these, like the DG Corporate Committee, DG Finance, and DG Science and Policy, were created or updated as part of a departmental governance review that was underway at the time of the audit. Others, such as the Project Management Advisory Committee and the DG Security Event Management Committee, were pre-existing structures.

Program branches also maintain or participate in various governance mechanisms that support their IT-related activities. Within the Meteorological Service of Canada (MSC), internal governance includes the MSC Change Approval Board, the MSC DG IT Oversight Committee, Director level IM/IT planning and operations related committee, and other working level related groups. Other branches maintain internal working-level groups such as the Environmental Protection Branch’s IM/IT Working Group and the Science and Technology Branch’s Directors IM/IT Committee.

ECCC also participates in interdepartmental forums related to the planning and operations of the HPC platform, such as the HPC Executive Renewal Committee, the HPC Solution Funding Proposal DG Steering Committee, and the HPC Management Advisory Committee. These committees are typically led or co-led by MSC and involve collaboration with other federal partners. Within ECCC, participation is primarily anchored in MSC, with additional representation from branches such as DSB, Science and Technology Branch and Corporate Services and Finance Branch, depending on the topic.

The Environment Protection Branch is a participant in the High Resilience Environment Steering Committee, which is led by another government department, and focuses on planning and oversight related to the continuity and availability of the High-Resilience Environment,

which supports the ECCC National Environmental Emergencies Centre and other partner departments-led high-availability operations.

Beyond departmental and interdepartmental committees, ECCC also engages in broader government-wide digital governance. For example, the Government of Canada Enterprise Architecture Review Board, where the Chief Service and Delivery Officer represents ECCC and participates in the review of departmental digital initiatives to ensure alignment with Government of Canada digital direction, priorities, and enterprise architecture standards. In addition, the Chief Service and Digital Officer participates in several horizontal governance forums that support strategic digital direction and cross-departmental coordination, including the CIO Council, the SSC CIO Roundtable, and the CIO Science Portfolio.

Effectiveness of Governance Bodies

The audit period coincided with a time of significant structural transition in ECCC's digital governance - marked by the creation and reorganization of DSB, a broader departmental governance review, a DSB led digital governance review, and ongoing updates to IM/IT governance at the program level.

As this transition was still underway at the end of the audit, the linkages between committees, their alignment with departmental priorities, and their roles within emerging governance models were still in the process of being defined. Several committees continued to operate concurrently in the absence of a cohesive structure, limiting the framework's ability to support effective decision-making and oversight. Some were operating under outdated or draft terms of reference, with mandates not yet aligned to the new corporate governance structure. Reporting linkages were inconsistently defined, and in some cases, it was unclear whether committees had been replaced, re-scoped, or remained active.

For example, the Digital Modernization Steering Committee (DMSC), led by DSB, was mandated to support the Deputy Minister in setting IM/IT investment priorities, including those requiring SSC involvement, and to endorse digital initiatives, projects, and investments. It was also responsible for aligning IM/IT and data priorities with financial management, project management, investment planning, and branch-level planning processes. The Committee reported to the ADM Operations Committee, referred endorsed initiatives to the Investment Management Committee for funding decisions, and served as an escalation mechanism for project issues that could not be resolved by lower-level governance bodies.

However, the Committee's terms of reference have not been updated to reflect the newly established Chief Service and Digital Officer and continued to reference linkages to the Project Management Advisory Committee and the Architecture Change Management Board, both of which listed the CIO as their lead. The DMSC's place within the revised departmental

governance structure remains unclear. IT and investment planning matters are now discussed in newly formed committees - DG Corporate and DG Finance - that support and report to the Executive Management Committee, and their terms of reference do not explicitly identify a connection to the DMSC.

The Architecture Change Management Board's terms of reference also stated that it reported to the rescinded ADM Operations Committee, leaving its role in the updated structure undefined. The Project Management Advisory Committee remained active as of March 2025. The audit team was informed that discussions were underway to redefine its role and responsibilities under a revised mandate to ensure proper accountabilities with respect to project management are met.

A review of Records of decision and committee documentation from the Architecture Change Management Board and the Digital Modernization Steering Committee showed limited effectiveness - evidenced by infrequent meetings, limited strategic challenge, and a high rate of automatic or conditional endorsements. Interviewees noted that participation often varied by branch interest and that these forums were viewed more as information-sharing platforms.

Interviews also confirmed that members were often unclear on their committee's mandate or reporting lines. In the absence of broader integration, there is a risk of reinforcing siloed decision-making and limiting the cross-functional perspective needed for strategic oversight.

Beyond corporate and DSB led governance, branches have also developed their own formal and informal governance structures to manage planning and operational aspects of IT. While these arrangements enable responsiveness to operational needs, they have evolved into parallel sub-processes that may not always reflect departmental priorities. Interviews and questionnaire responses indicated that branches typically consolidate their directorate-level needs before submitting proposals as part of the DSB-led investment process. DSB officials noted concerns that such decentralization limit visibility and oversight at the enterprise level.

Overall, the audit found that the Department's IT governance environment lacks cohesion. Fragmentation and unclear linkages across governance bodies increase the risk of siloed decision-making, duplicative efforts, and reduced enterprise visibility. This affects the Department's capacity to manage cross-cutting risks, align with government-wide digital priorities, and coordinate effectively with service providers such as SSC. It also constrains ECCC's ability to provide consistent oversight of emerging areas such as artificial intelligence AI, data-driven innovation, and the responsible adoption of enabling technologies. Without integrated governance mechanisms, initiatives may advance without appropriate challenge, alignment, or risk-informed decision-making.

This challenge is particularly acute in areas like environmental prediction and mission-critical services, where ECCC's operations depend on continuous access to external and internationally sourced data. Given the Department's reliance on a complex web of digital infrastructure, external partners, and geopolitical dynamics, reinforcing data governance - through clear roles, integrated oversight, and proactive enterprise coordination - will be important to sustain performance, innovation, and resilience.

Roles and responsibilities

The audit found that roles and responsibilities for IT governance remain inconsistently defined and operationalized. For example, a 2019 Memorandum of Understanding (MOU) between the Corporate Services and Finance Branch and two program branches (MSC and Science and Technology Branch), continues to govern IM/IT service delivery related to high performance and scientific applications - despite structural changes, evolving governance requirements, and the creation of DSB.

Under the MOU, operational management of IT functions related to high performance and scientific applications - including application development and support services - remains with the branches, while DSB is responsible for functional direction, liaison with SSC for infrastructure, business intake, desktop support, and framework for Authority to Operate process for applications. This arrangement has resulted in a dual model where accountability for enterprise-wide IT-related activities is fragmented.

The evolving relationship between the ECCC Chief Service and Digital Officer, as the departmental Designated Official for Service Management, and program ADMs who act as service owners for IT-enabled services has not yet been clearly defined. While the Policy on Service and Digital distinguishes between enterprise direction and service delivery accountability, departmental governance documents and structures do not clearly articulate how these roles interact. It remains unclear how responsibilities for service performance, digital modernization, and risk escalation are expected to be shared. This raises questions about accountability - particularly in the event of a failure or disruption involving a mission-critical IT-enabled service - regarding whether responsibility would rest with the Chief Service and Digital Officer or the responsible program ADM.

Additionally, the current model does not provide clear visibility and escalation mechanisms across IT domains such as cyber security, local solution management, architecture, incident management, or disaster recovery and business continuity management. The SSC liaison function, established in DSB, was still evolving at the time of the audit and had not yet been consistently leveraged or embedded in governance processes.

The absence of a comprehensive and updated governance framework may also contribute to the lack of clarity in roles and responsibilities. Although DSB is responsible for establishing enterprise direction, it has not implemented a clearly defined suite of departmental policies, standards, or internal instruments that articulate how digital and IT requirements should be applied in practice, in alignment with the Policy on Service and Digital and related instruments.

For example, in the case of AI-related direction and strategies, work was initiated by program branches in response to emerging needs and evolving policy context, with limited early engagement from DSB. While this reflects branch responsiveness and innovation, it also illustrates the risks of enterprise direction being outpaced by decentralized action. Similar findings with respect to the lack of a departmental-wide framework, policies, standards, and guidance were raised in a separate internal audit, with respect to cyber security and the management of local solutions.

As the Department will increasingly leverage technologies like AI, cloud platforms, and advanced analytics to deliver on its mandate, the need for clear accountabilities, enterprise oversight, and effective coordination becomes more pronounced. Ensuring that governance structures are equipped to support these shifts will be critical to maintaining alignment with the evolving digital context.

Recommendation 1: As part of the work already underway to support the re-organization of the Digital Services Branch, the ADM, Chief Service and Digital Officer, DSB, in collaboration with other branches as appropriate, should continue reviewing and strengthening the departmental IT governance framework. This includes further clarifying accountabilities, such as those related to service management, along with mandates and linkages of governance bodies, updating terms of reference, and refining coordination mechanisms across enterprise and branch-level structures, in alignment with the Policy on Service and Digital and the evolving digital operating context.

Management Response:

The ADM, DSB agrees with the recommendation.

The recommendation will be addressed through two streams in parallel, including a review of existing governance and a review of all seminal policy requirements to ensure the appropriate governance approach and alignment within the Department, while also better leveraging other approaches to enhance communication such as communities of practice and working groups.

2.2. Enterprise IT planning and prioritization

Key findings: ECCC has established a departmental process for IT investment planning and prioritization that aligns with TB requirements, and has made progress in strengthening strategic service functions, such as digital costing. There is an opportunity to strengthen the integration with other departmental planning functions.

The current differences in timelines, criteria, and oversight between IT and capital planning processes reduces the Department's ability to align investments with enterprise priorities. There is an opportunity to enhance coordination in support of a shared understanding of priorities and to ensure that IT investment decisions align with enterprise-wide digital objectives.

What we examined

The audit assessed the extent to which ECCC has established integrated, strategic, and effective processes to plan and prioritize IT investments, in alignment with the TB Directive on Service and Digital.

This included examining whether IT investments are prioritized based on departmental needs and enterprise objectives, and whether planning processes are coordinated across the department to support a comprehensive and risk-informed view of IT investment decisions.

What we found

DSB has established departmental processes to support enterprise-wide IT planning and prioritization, aligned with TB's Prioritization Framework and the Policy on Service and Digital. This includes the development of ECCC's Enterprise Prioritization Framework, which uses risk and capability-based criteria such as urgency, business continuity, cybersecurity, and funding availability to assess IT investment proposals across branches.

As part of this process, each branch designates a Branch Digital Investment Lead, who is responsible for coordinating internal proposals and liaising with DSB throughout the year. While this structure provides a foundation for enterprise IT governance, the audit identified a risk that lower-priority proposals not selected through the enterprise process may proceed informally. These proposals may fall outside of enterprise oversight and contribute to the ongoing proliferation of local solutions—potentially undermining standardization efforts, integration, and cyber security objectives. To address this risk, DSB has introduced the Digital Service Accelerator Program to enable the realization of lower-priority projects through a

centralized service offering. However, the audit noted that additional controls may be needed to improve visibility over unfunded or unapproved proposals.

The audit also identified a disconnect between the IT investment demand process (led by DSB) and the departmental capital planning process (led by the Corporate Services and Finance Branch). Each is led by separate teams in different branches using different prioritization criteria, different reporting timelines, and governance structures. As a result, there is no mechanism to assess IT investment and capital asset proposals against a common enterprise view. This creates challenges in aligning funding with departmental priorities and may reduce the Department's ability to strategically manage its digital assets.

Efforts have been made to enhance the capital planning process by designating IM/IT asset category leads, responsible to provide advice and recommendations to branches on IM/IT projects, hardware, and licenses, to communicate what items are on the IM/IT priority lists to Branches and FMAs, and to make decisions on approving or not the capital plans submitted by branches under the asset categories IM/IT hardware and IM/IT.

DSB has made progress in building costing capacity to support funding submissions. The Digital Costing team within the DSB has been building capacity and expertise to provide accurate, timely, and comprehensive cost estimates for departmental IT funding requests. However, challenges remain in generating reliable data for internal service estimates. Reported historical underfunding of IT services and reliance on outdated assumptions have limited the accuracy of forecasts, and stakeholders indicated that costing practices for digital services remain inconsistent. These limitations reduce the quality of information available to support effective planning, prioritization, and decision-making, key elements of governance as set out in the Policy on Service and Digital.

Overall, while foundational IT investment planning structures are in place, the audit found that integration with broader departmental planning remains limited. Further improvements are needed to align planning functions, enhance oversight of non-prioritized solutions and ensure that IT funding decisions reflect strategic priorities and enterprise risk. These needs are especially relevant in the current context of fiscal pressures and government-wide efforts to streamline operations and improve efficiency. Strengthening alignment - particularly between capital and IT investment planning - will be key to optimizing the value of digital investments and ensuring governance decisions are both strategic and resource-informed. This said, we recognize that the different timelines associated with each process as dictated by TBS make this challenging.

Recommendation 2: As part of continuing to support the department's digital transformation journey, the ADM, Chief Service and Digital Officer, DSB, should continue working with the ADM, Corporate Services and Finance Branch, to enhance alignment between departmental IT investment planning and capital planning processes. This includes enhancing and refining information sharing mechanisms, further integrating prioritization approaches into a singular enterprise approach, and improving visibility over IM/IT-related capital requirements, supporting more integrated and risk-informed planning in line with enterprise IT governance objectives.

Management Response:

The ADM, DSB agrees with the recommendation.

The recommendation will be addressed through a detailed review of the existing processes, a review of the different policy requirements for IT investments and supporting the development of a holistic process that incorporates digital into the broader enterprise investment planning. The broader enterprise investment planning process is managed by the Corporate Services and Finance Branch.

2.3. Administering ECCC's relationship with SSC

Key findings: ECCC has established mechanisms to support its relationship with SSC, including a liaison function within DSB. As the department continues its digital transformation, there is more work to do with respect to how the department interacts with SSC, and to better define oversight of service agreements. At the time of the audit, several agreements that branches had with SSC were not included in the liaison office's list, and many of those agreements were missing key elements such as defined roles, performance expectations, and dispute resolution processes.

There were opportunities for improvement identified to strengthen the governance that supports the department's interactions with SSC, including continuing work to clarify roles and responsibilities, and enhance enterprise visibility for the support provided to deliver mission-critical operations.

What we examined

The audit assessed the extent to which ECCC has established governance structures and oversight mechanisms to effectively manage its relationship with SSC. This included examining

whether the Department had clear roles, responsibilities, and processes in place to coordinate service requests, monitor service delivery, and provide enterprise-level visibility and direction. The audit also considered whether internal stakeholders understood their responsibilities in engaging with SSC, and whether mechanisms existed to support prioritization, decision-making, and accountability for services provided by SSC.

What we found

Central coordination

DSB has established a central coordination function, the SSC Liaison Office, to facilitate service requests and function as the main point of contact with SSC. The unit, composed of one manager and four full-time employees, supports internal clients and helps coordinate departmental needs with SSC.

At the time of the audit, the Liaison Office remained an emerging function. It did not oversee all SSC-related interactions across the Department, and there were no formal procedures, defined roles, or a clear mandate governing its operations. Interviews confirmed that awareness of the Liaison Office's role was limited, with most branches relying on informal relationships with DSB colleagues to support SSC engagements. Although most branches said they would contact DSB for SSC-related matters, few specifically referenced the SSC Liaison Office.

The Liaison Office also does not currently track or analyze the types of services requested from SSC. This information could support departmental planning and enable the identification of enterprise-wide needs, funding requirements, and local solution risks, for example, if a branch declines an SSC service proposal and pursues its own alternative.

Service Agreements

Departments acquire SSC services through standard Service Agreements, which outline costs, service terms, and responsibilities. The audit found that oversight of these agreements at ECCC is decentralized, and that the department lacks a consolidated and up-to-date inventory.

In 2024, DSB, with support from its financial management advisor, identified 36 active SSC service agreements totaling approximately $7.3 million. The audit found additional agreements that were not captured in this list, indicating gaps in departmental tracking. Historically, branches committed funding directly to SSC, but the process has since shifted: SSC now invoices DSB centrally for all services, underscoring the need for centralized oversight.

The audit examined a judgmental sample of seven (7) service agreements. While the sample size limits generalization across the total population, it highlighted recurring issues:

- Of the four agreements drawn from the consolidated inventory, none included defined roles and responsibilities, performance measures, or escalation mechanisms. All were signed by DSB officials.
- One agreement, covering the HPC platform, was not included in DSB's inventory. Though it contained key service level expectations and technical details, it had not been updated since 2015, lacked ECCC signatures, and it was unclear who was responsible for updates to the service agreement.
- Two agreements supporting the High Resilience Environment were also missing from the inventory and did not include basic terms such as roles, performance metrics, or dispute resolution processes.

The lack of a comprehensive and current inventory, combined with inconsistencies in agreement content and ownership, poses risks to the Department's ability to ensure service quality, monitor performance, and address issues with SSC. As dependencies on SSC services grow, the Department will need to strengthen its coordination mechanisms, clarify internal responsibilities, and ensure agreements are tracked, maintained, and enforced in alignment with enterprise-level governance.

IT-enabled mission-critical operations

As part of the analysis of how ECCC manages its relationship with SSC, the audit examined governance arrangements for two mission-critical, IT-enabled services. In both cases, the continued delivery of these services, on behalf of the Department to Canadians and other organizations, relies heavily on SSC-provided IT infrastructure and solutions.

Governance for High Resilience Environment-enabled mission-critical services

The National Environmental Emergencies Centre, within the Environmental Protection Branch, provides 24/7 operational support for environmental emergency response. To ensure service continuity, it relies on the High Resilience Environment, a specialized Infrastructure-as-a-Service solution provided by SSC. ECCC is one of five departments participating in this platform, with coordination led by the National Environmental Emergencies Centre and approximately $250,000 committed in departmental funding over three fiscal years. Strategic oversight is provided through an interdepartmental steering committee, chaired by the lead department.

In this arrangement, the lead department has established two service agreements with SSC, one for internet bandwidth and one for data centre rack space, on behalf of all participating departments. ECCC is not listed as a direct client under these agreements, and the

arrangement is not reflected in the DSB's inventory of service agreements or associated coordination mechanisms. At the time of the audit, the branch was not directly involved in managing the relationship, and interviews indicated that the centre interacted with SSC through informal channels to address operational needs.

While this approach has enabled responsiveness to operational requirements, it also highlights a broader challenge related to enterprise visibility over services that depend on external infrastructure. Without a clear view of departmental dependencies or formal mechanisms for risk escalation, governance structures may be limited in their ability to support continuity planning or align operational arrangements with enterprise priorities. As ECCC continues to strengthen its governance of services reliant on SSC, ensuring greater visibility and coordination for these types of arrangements may help reinforce accountability and operational resilience.

Governance for HPC-enabled mission-critical services

Weather-related services, led by MSC, represent one of the most complex IT-enabled operations at ECCC. These services - which include weather forecasts, warnings, air quality predictions, and other environmental information - support public safety, economic activity, and decision-making across Canada. These services rely on a highly specialized chain of technology systems to run science models, process massive amounts of data, and provide reliable information to Canadians and government partners - 24 hours a day, 7 days a week.

Several teams across ECCC - and beyond - contribute to the delivery of these services and depend on the work of multiple branches responsible for designing, testing, deploying, and running hundreds of software applications and models. Together, these tools support the collection, processing, and dissemination of data, as well as the infrastructure and networks required to sustain uninterrupted operations.

- MSC's Canadian Centre for Meteorological and Environmental Prediction and the Science Technology Branch's Atmospheric Sciences Division lead research and development to improve forecasting models and environmental prediction systems. Once validated, these systems are transitioned into production, with this development-to-operations cycle managed within MSC.
- DSB supports MSC through its Applied Sciences Applications Division, which is responsible for managing and maintaining the specialized, mission-critical systems used for real-time scientific processing, including: scientific architecture design and real-time software development, tools for managing climate archive data, software for processing and visualizing meteorological and satellite data, support for mobile weather applications and 24/7 system operations in collaboration with SSC, etc. These services are provided based on MSC's needs and are prioritized according to available

resources and internal capacity and formalized through a Service Level Agreement between DSB and MSC.

The outputs of this development, whether scientific models, software tools, or data pipelines, are then used by other operational teams in MSC to process and deliver final forecast products and services to the public and specialized clients.

- Prediction models run on the Government of Canada's HPC platform, which includes two of the most powerful supercomputers in the country. SSC is responsible for managing the overall environment, including IT systems, networks, telecommunications, and middleware. SSC provides these services through a Service Agreement with ECCC.
- The HPC platform itself is hosted by a third-party vendor under a contract managed by SSC. The vendor is responsible for delivering technology upgrades every 30 months to ensure ongoing performance and capacity. These upgrade cycles are complex and require detailed planning and coordination between SSC and ECCC to ensure operational continuity.

The service model that supports these mission-critical operations has evolved significantly over time. Historically, MSC managed both the scientific systems and much of the supporting infrastructure in-house. The creation of SSC in 2011 marked a shift to a centralized model for infrastructure services, including the transfer of key personnel and the HPC infrastructure from MSC to SSC.

This transition has maintained operational continuity, in part due to longstanding relationships between technical teams and their physical co-location. However, over time, the landscape has evolved significantly – structural changes, loss of institutional knowledge and workforce transition, the broader transformation of the federal service and digital landscape, shift in strategic priorities and vision towards an enterprise vision for service and digital, have made this model increasingly complex and harder to manage within the original assumptions.

Recent policy developments, such as the Government of Canada's Digital Ambition and the Policy on Service and Digital, have introduced new expectations related to service integration, enterprise accountability, and the designation of departmental officials responsible for digital oversight. At ECCC, this includes the creation of DSB and the formal designation of the Chief Service and Digital Officer, whose mandate encompasses both IT governance and service management, reporting directly to the Deputy Minister.

Concurrently, SSC's Enterprise 3.0 Strategy is driving further transformation of legacy infrastructure in support of whole-of-government digital priorities. While ECCC remains the main client of the high-performance computing platform, the infrastructure is now considered a

Government of Canada enterprise asset managed by SSC. This separation of operational control from service accountability introduces a degree of risk that is not fully addressed in current governance tools, particularly as digital transformation accelerates, and dependencies deepen.

SSC-led initiatives, such as enterprise data centre consolidation and infrastructure standardization have downstream effects on HPC operations. While these projects support SSC and GC long-term digital goals like accessibility, availability, capacity, and predictability, they also introduced short term operational challenges for ECCC. These include legacy system migration challenges, unplanned workloads for ECCC staff to support the SSC-led projects, and service outages that have affected continuity of operations. These issues underscore the need for governance mechanisms capable of managing cross-jurisdictional dependencies and shared service risks.

We noted that ECCC has put in place various governance structures to manage its relationship with SSC, and to support planning and operations continuity, largely established and or led by MSC. DSB representatives have been engaged in these structures and are contributing to enterprise-level review processes such as the GC Enterprise Architecture Review Board:

- Governance for HPC Renewal**.** The contract with the third-party vendor is set to expire in 2028. SSC and ECCC are working on the HPC renewal project to enhance the capacity of the current infrastructure and prepare it for the next HPC version, as well as procuring a new hosting vendor contract. The renewal of the next HPC solution is supported by tiered, interdepartmental committee governance model with the following key bodies:
    - ADM-level Executive Committee (co-chaired by ECCC and SSC)
    - DG-level Steering Committee (supports the Executive Committee)
    - Working groups (focused on project by executive and director-level committees and various supporting working groups).

  The focus of these governance mechanisms is to support the third-party independent review using TBS Independent Review Program, to specify HPC requirements and options, and to develop a proposal clearly identifying the requirements, options and costing to ensure securing funding levels, a source of funds and funding authorities.

- Governance for non-mission-critical use of HPC resources**.** The HPC infrastructure also includes an environment that supports non-mission-critical science related activities. A joint HPC Governance committee manages allocation of HPC resources to a variety of stakeholders (which are used by several departments other than ECCC), prioritizing workloads based on ongoing operational requirements and departmental priorities.

Basically, the ECCC experts that use the HPC for mission-critical activities also prioritize and manage the allocation of HPC resources for non-mission-critical activities.

- Governance for MSC IM/IT planning and operations. Several governance bodies exist in MSC to manage IM/IT planning and operations and have been updated via a MSC IM/IT governance review in 2024. These include an MSC DG IT Operations Committee, the MSC Change Approval Board, director sub-committees and other working level mechanisms.

  A Quality Management System (QMS) Steering committee is also in place, mandated to provide senior management oversight and guidance for maintaining and strengthening the QMS. It is chaired by the ADM MSC and membership includes all MSC DGs, the Chief Service and Digital Officer and SSC HPC director.

- QMS processes and Service Level Agreements. Business processes for IT-enabled weather services and associated controls such as roles and responsibilities of all stakeholders are documented, followed, and monitored as part of the MSC Quality Management System. HPC services provided by SSC are formalized in a Service Agreement between SSC and ECCC. Services provided by DSB are documented in a Service Agreement between DSB and MSC.

Challenges and opportunities for improvement

The audit identified several challenges and opportunities for improvement related to the current governance of HPC supported mission-critical IT services.

These foundational governance tools, originally designed around the 'MSC enterprise' model, reflect a structure in which MSC is positioned at the center of service delivery, with other key players such as SSC and internal ECCC partners positioned as supporting or enabling entities. This reflects the operational reality and complexity of MSC's mandate. However, the design of these governance mechanisms has not fully adapted to align with the shift toward departmental and Government of Canada enterprise structures. As set out in the Policy on Service and Digital and related federal priorities, service delivery is increasingly governed through shared accountabilities and integrated oversight.

The Service Agreement between ECCC and SSC has not been updated since 2015, and key QMS processes - such as those related to incident management - have not been revised to reflect current roles and responsibilities across all stakeholders. A review of meeting minutes and meeting materials from the various committees suggests that efforts have been made to integrate the DSB into MSC-led structures. However, the practical value and fit of DSB's involvement remains unclear.

Governance documents and committee records do not fully reflect the evolving relationship between the Chief Service and Digital Officer - designated as the departmental service management lead - and the ADM responsible for MSC, who acts as the service owner for weather-related operations. How these two roles work together in the context of digital modernization has yet to be clearly articulated.

MSC's and Science and Technology Branch's research and innovation processes involve experimental or parallel runs of new or updated modeling systems, which are later transitioned into production following internal QMS validation. These activities are led independently within MSC and are not integrated into broader departmental oversight mechanisms. This points to the need to ensure that a solid framework is in place to mitigate cybersecurity risks and to ensure appropriate controls are being applied in line with the Policy on Service and Digital - which places accountability for departmental IT and cybersecurity with the CIO and the Designated Official for Cyber Security in DSB.

In terms of interactions with SSC, multiple formal and informal points of contact exist between SSC, DSB, and MSC - ranging from structured liaison functions within DSB to direct technical and operational engagement between SSC and MSC teams. These numerous pathways reflect the complexity of the current service delivery model but also raise concerns regarding consistency, accountability, and coordination.

Interviews with stakeholders from both DSB and MSC highlighted difficulties in planning and communicating with SSC, along with a broader need to clarify roles and responsibilities within ECCC. Recent infrastructure and application incidents affecting the continuity of 24/7 operations further underscored these challenges. In response, an Incident Management Task Team was established in 2022, bringing together SSC, MSC, and DSB to assess vulnerabilities in mission-critical IT services. The team identified unclear escalation processes, incomplete incident response protocols, and gaps in operational governance.

Taken together, these findings point to a governance model that remains in transition. Long-term planning activities, such as HPC renewal, have benefited from more structured engagement and growing participation by the DSB. However, the governance supporting ongoing IT operations has not yet fully adapted to the Department's integrated and interdependent operating context and the emerging risks. As the Department continues to adapt to enterprise-wide digital transformation and evolving expectations under the Policy on Service and Digital, there is a need to clarify governance roles and strengthen coordination mechanisms to ensure continuity, accountability, and readiness for future challenges.

Recommendation 3: As part of the ongoing transformation and maturation of the Digital Services Branch, the ADM, Chief Service and Digital Officer, DSB, in collaboration with the ADM, MSC, and other relevant stakeholders, should continue reviewing and strengthening governance mechanisms for SSC-dependent, mission-critical digital services considering the support model that is being implemented within the Digital Services Branch. This includes clarifying internal roles and accountabilities for service oversight, incident response, cybersecurity, and coordination with SSC - ensuring alignment with the Policy on Service and Digital and Government of Canada's evolving digital strategies.

Management Response:

The ADM, DSB agrees with the recommendation.

The recommendation will be addressed through a review of all mission-critical services, the associated solutions, to ensure an understanding of their linkages and health, and the development of an incident response framework including detailed roles and responsibilities (or changes to existing responsibilities) to ensure clarity on the incident management coordination between MSC, SSC and DSB.

3. Conclusion

The audit found that ECCC has taken meaningful steps to modernize its IT governance framework and align with the Government of Canada's Policy on Service and Digital. The establishment of DSB, the designation of key digital leadership roles, and the implementation of planning mechanisms reflect real progress. These foundational changes provide an opportunity to move toward more integrated oversight, clearer accountability, and enterprise-level alignment.

At the same time, IT governance across the Department still has opportunities for improvement to address overlapping mandates, inconsistent oversight, and limited visibility over IT-enabled operations and SSC-dependent services. These areas should be addressed to enhance ECCC's ability to manage cross-cutting risks, support timely decision-making, and ensure IT investments and digital operations support both departmental objectives and government-wide priorities.

The current digital transformation taking place within ECCC is important because looking forward, the Department's ability to govern digital services will increasingly shape its capacity to deliver on its mandate and priorities. Emerging technologies such as AI, advanced analytics,

and supercomputing are reshaping how science and policy intersect, while global shifts in cybersecurity, data governance, and digital sovereignty raise new considerations for risk, compliance, and trust. As a science-based department, ECCC is uniquely positioned to play a key role in these areas. Doing so will require a cohesive governance framework that enables innovation while ensuring security, interoperability, and accountability across a complex digital ecosystem.

As the ADM DSB continues to focus on strengthening coordination, clarifying accountabilities, and reinforcing enterprise oversight, these areas will help ECCC navigate this evolving landscape with agility and long-term perspective - particularly amid fiscal pressures, growing interdependencies in service delivery, and the need to ensure resilient access to critical data and digital infrastructure in a shifting geopolitical context.

4. Appendix A – Audit Criteria

1.1 Governance structures are in place, documented, and operate effectively to enable decision-making, and support oversight and accountability for IT-related activities.

1.2 Roles, responsibilities, and accountabilities for IT governance across the department are clearly defined, communicated, and understood.

1.3 A framework is in place to effectively administer the enterprise level relationship with SSC.