Audit of NRCan’s risk management practices

Presented to the Departmental Audit Committee (DAC)

February 13, 2025

On this page

Executive summary

Introduction

Risk management [1] is a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, making decisions on and communicating risk issues. Effective risk management practices enable organizations to make informed decisions amidst rapidly evolving risk landscapes and environments. It also helps nurture a positive risk culture throughout the organization that empowers individuals to routinely consider how risk impacts their day-to-day activities and to embed risk management principles into their work. Risk culture [2] refers to the attitudes and behaviours found within an organization that are associated with risk management. This includes elements such as whether an organization views risk management as an inherent part of good decision-making, or simply as a reporting requirement; whether an organization tends to be risk averse, or views risks as including potential opportunities; and whether risk management is embedded at all levels of an organization or is a top-down process only. Risk appetite [3] is a broad description of the type and amount of risk an organization is willing to pursue or accept in pursuit of its objectives. It is generally set by senior management. Risk tolerance is the specified range of acceptable results within the organization's risk appetite. Risk tolerance indicates the sensitivity to risks of an organization or a project or program. It is typically determined at the project and program level.

Within the Government of Canada, risk management activities are guided by the Treasury Board (TB) Framework for the Management of Risk (the Framework), and the Guide to Integrated Risk Management – a Recommended Approach for Developing a Corporate Risk Profile (CRP). This Framework and associated guidance came into effect August 27, 2010.

Although the Framework and associated guidance provide direction to departments to ensure that organizations are managing risk effectively, departments are not required to comply with these instruments. In June 2023, NRCan’s 2023-2026 CRP was formally approved by senior management. The CRP is intended to be leveraged to inform the Department’s decision-making activities related to priority setting, strategic direction, and resource allocation.

At Natural Resources Canada (NRCan), the Strategic Planning, Risk and Reporting Division (SPRR) within the Planning, Delivery and Results Branch of the Strategic Policy and Innovation Sector (SPIS) is responsible for supporting the implementation of corporate risk management practices within the Department. Sectors are responsible for implementing sector- and program-level risk management processes as applicable to their day-to-day operations. The SPRR Division is currently refreshing the Departmental Integrated Risk Management Policy Framework. The previous iteration of NRCan’s Integrated Risk Management Policy Framework came into effect in June 2015.

While the SPRR Division oversees and provides guidance to sectors on NRCan’s overarching, corporate-level risks, sectors identified as risk leads during the CRP development are responsible for managing, monitoring, and reporting on their respective risk areas. Beyond the CRP, sector and program personnel are responsible for risk management in their respective areas, including the identification, assessment, management, and monitoring of risks. To that end, sector and program personnel are responsible for implementing their own risk management practices, tools, and guidance.

The objective of this audit was to assess whether the Department has established effective processes to ensure the implementation and integration of sound risk management principles in support of achieving its objectives.

Strengths

Overall, the Department has governance committees to provide oversight and strategic direction on integrated risk management. These committees also serve as communication and collaboration mechanisms for horizontal risk discussions at the senior management level. There is some strategic guidance and direction for departmental risk management, including a Corporate Risk Profile that outlines the strategic and operational risks faced by the Department, a draft Integrated Risk Management Framework to guide the establishment and management of the Corporate Risk Profile, and a draft Departmental Risk Management Strategy that outlines the Department's overall approach for risk management. Some risk management principles are being applied in the sectors and is formalized and most evident for transfer payment programs to meet requirements of the Treasury Board submission process.

Areas for improvement

There are opportunities to strengthen the Department's risk culture by establishing the Department's risk appetite and tolerance, clarifying roles and responsibilities of key players for risk management within the Department, finalizing and communicating guidance documents for departmental risk management, and leveraging existing risk management training resources and materials for raising awareness, building capacity, and better equipping employees in applying risk management principles in day-to-day activities.

The impact of not addressing these areas for improvement is that the Department may not be equipped and prepared to identify, assess, and mitigate existing, new, and emerging risks in a timely manner, putting the Department at risk of not meeting its objectives.

Internal audit conclusion and opinion

In my opinion, the Department has some governance mechanisms and processes in place to support the implementation and integration of risk management principles, including several strategic and guidance documents and tools for departmental risk management. There is also coordination and collaboration across the Department for the development of these documents and tools. The audit has identified opportunities to strengthen the Department's risk culture, and to formalize and communicate risk management principles for employees to apply in their day-to-day activities beyond the Corporate Risk Profile exercise.

In order to establish a strong corporate culture that is risk aware and views risk management as an inherent part of good decision-making, NRCan must ensure that it anticipates and plans for the impacts of potential negative events it foresees. Risk management cannot be done in silos, or from a top down only or bottom up only approach. There is a need to avoid a disconnect between corporate risks and the operationalization of risk management at the working level, which can hinder the Department from responding to, and actively anticipating and preparing for new and emerging risks on the horizon. Risk should not be viewed only in terms of probability and impact; the Department must consider risk velocity, how fast a risk exposure can negatively impact the Department. Being reactive rather than proactive to risk events when they occur can expose the Department to impacts by known and unknown risk events that could occur.

Defining and communicating risk tolerance and risk appetite is critical to fostering a proactive risk management culture, ensuring strategic alignment, and building stakeholder trust. By clearly articulating these concepts, the Department can navigate uncertainties more effectively and enhance its overall resilience and adaptability to change. The absence of clearly defined risk tolerance and risk appetite can lead to challenges and some detrimental outcomes. Without these essential frameworks, decision-makers may struggle to evaluate potential risks effectively, leading to inconsistent approaches to risk management across the Department.

Statement of conformance

In my professional judgement as Chief Audit and Evaluation Executive, 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 engagement supervision and the Quality Assurance and Improvement Program.

Michel Gould, MBA, CPA, CIA

Chief Audit and Evaluation Executive

February 13, 2025

Acknowledgements

The audit team would like to thank those individuals who contributed to this project and, particularly employees who provided insights and comments as part of this audit.

Introduction

Risk management [4] is a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, making decisions on and communicating risk issues. Effective risk management practices enable organizations to make informed decisions amidst rapidly evolving risk landscapes and environments. It also helps nurture a strong risk culture throughout the organization that empowers individuals to routinely consider how risk impacts their day-to-day operations and to embed risk management principles into their work. In public service administration, effective risk management practices contribute to an improved allocation of time and resources, ultimately providing better results for Canadians. Risk culture [5] refers to the attitudes and behaviours found within an organization that are associated with risk management. This includes elements such as whether an organization views risk management as an inherent part of good decision-making, or simply as a reporting requirement; whether an organization tends to be risk averse, or views risks as including potential opportunities; and whether risk management is embedded at all levels of an organization or is a top-down process only. Risk appetite [6] is a broad description of the type and amount of risk an organization is willing to pursue or accept in pursuit of its objectives. It is generally set by senior management. Risk tolerance is the specified range of acceptable results within the organization's risk appetite. Risk tolerance indicates the sensitivity to risks of an organization or a project or program. It is typically determined at the project and program level.

Within the Government of Canada, risk management activities are guided by the Treasury Board (TB) Framework for the Management of Risk, and the Guide to Integrated Risk Management – a Recommended Approach for

Developing a Corporate Risk Profile (CRP). This Framework and associated guidance came into effect August 27, 2010. Although the Framework and associated guidance provide direction to departments to ensure that organizations are managing risk effectively, departments are not required to comply with these instruments.

At Natural Resources Canada (NRCan), the Strategic Planning, Risk and Reporting Division (SPRR) within the Planning, Delivery and Results Branch of the Strategic Policy and Innovation Sector (SPIS) is responsible for supporting the implementation of corporate risk management practices at the Department. The SRPR Division supports various risk management activities, including the development and implementation of the CRP, the drafting of a Departmental Integrated Risk Management Policy Framework, reviewing corporate level risk on key files relating to reporting, and acting as a functional reviewer with a risk lens for TB submissions and Memoranda to Cabinet. All these actions are intended to support the fostering elements of a strong risk culture that permeates through all NRCan activities.

In June 2023, NRCan's 2023-2026 CRP was formally approved by senior management. The CRP was developed collaboratively with input obtained from NRCan sectors, corporate governance committees, and senior management, and outlines the Department's main strategic and operational risks, as well as accountabilities, existing controls, and planned mitigation strategies. In support of the CRP, NRCan has developed and piloted a risk monitoring approach that will support the Integrated Business Planning process. At the same time, risk leads are being engaged directly to gain a full perspective of each risk, including the implementation status for mitigation strategies across the Department. The CRP is intended to be leveraged to inform the Department's decision-making activities related to priority setting, strategic direction, and resource allocation.

The SPRR Division is also currently in the process of refreshing the Departmental Integrated Risk Management Policy Framework. The previous iteration of NRCan's Integrated Risk Management Policy Framework came into effect in June 2015. To effectively manage risk, organizations may develop and implement a risk management framework that defines roles and responsibilities, organizes activities, outlines resource allocations, and describes reporting and monitoring mechanisms. An organization's risk management framework provides the necessary guidance to ensure that risks are proactively managed at every level and across all significant activities and functions of the organization.

While the SPRR Division oversees and provides guidance to sectors on NRCan's overarching, corporate-level risks, sectors identified as risk leads during the CRP development are responsible for managing, monitoring, and reporting on their respective risk areas. Beyond the CRP, sector and program personnel are responsible for risk management in their respective areas, including the identification, assessment, management, and monitoring of risks. To that end, sector and program personnel are responsible for implementing their own risk management practices, tools, and guidance.

This audit was included in the 2023 – 2028 Integrated Audit and Evaluation Plan, approved by the Deputy Minister on April 25, 2023.

Audit purpose and objectives

The objective of this audit was to assess whether the Department has established effective processes to ensure the implementation and integration of sound risk management principles in support of achieving its objectives.

Specifically, the audit assessed whether:

- The Department has adequate and effective governance mechanisms in place to support the integration of risk management practices and principles across the Department;
- The Department has adequate and effective practices in place to enable communication and coordination of risk management principles and activities across the Department; and
- Sound risk management principles are being effectively applied within the Sectors.

Audit considerations

A risk-based approach was used in establishing the objectives, scope, and approach for this audit engagement. A summary of the key underlying potential risks identified during the planning phase include:

- Adequate and effective governance mechanisms are necessary to facilitate strategic and operational risk discussions and information sharing across all levels of the Department;
- Adequate roles, responsibilities, and accountabilities are required to ensure that all parties are aware of their expectations relating to risk management;
- Adequate training and guidance are essential to ensuring that risk management concepts are well understood and can be integrated across all levels of the Department;
- Effective coordination processes are necessary to enable adequate sharing and gathering of pertinent risk information across the Department;
- Communication mechanisms are required to enable the use of key information in support of timely decision-making; and
- Effective tools and guidance need to be present to ensure that Sector representatives are able to integrate proper risk management principles

into their projects and programs.

Scope

The scope of this audit focused on activities and processes supporting NRCan’s risk management practices, between May 2022 and June 2024, with a focus on more recent activities. The audit examined governance mechanisms, communication and coordination practices, and training, guidance, and tools in support of NRCan’s risk management practices. The audit did not conclude on the appropriateness of specific, individual risks identified within the CRP or through other departmental risk management activities; rather, the focus was on the existence and adequacy of the processes themselves. Additionally, the audit did not assess the appropriateness of the mitigation measures that were established and implemented to manage individual risks identified.

The results of previous audit and evaluation projects on related topics were considered to inform the audit and reduce duplication of efforts.

A judgmental sample of Sectors and Programs were selected for detailed analysis, ensuring a thorough review while optimizing resources and focusing on areas of significant impact within the Department.

This audit did not examine AEB’s own contributions to risk management at NRCan. This exclusion was necessary to maintain the objectivity and independence required for an unbiased assessment of the organization's risk management practices.

Approach and methodology

The approach and methodology followed the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* and the Government of Canada’s *Policy on Internal Audit*. These standards

require that the audit be planned and performed in such a way as to obtain reasonable assurance that audit objectives are achieved. The audit included tests considered necessary to provide such assurance. Internal auditors performed the audit with independence and objectivity as defined by the *International Standards for the Professional Practice of Internal Auditing*.

The audit included in the following key tasks:

i. Interviews with key SPIS personnel and a selection of risk leads;
ii. Conducting a department-wide survey on risk management to all employees to obtain employees' perspectives on risk management and to analyze trends on risk management awareness. The survey was sent to all employees excluding AEB staff (approximately 5,700 employees). It was administered over a period of 30 days and received 480 responses (response rate of 8.4%);
iii. Review of key documents and select business processes in support of risk management including the Corporate Risk Profile, the draft Integrated Risk Management Framework, and the draft Departmental Risk Management Strategy;
iv. Review of available risk management guidance and training materials from the Treasury Board of Canada Secretariat and the Canada School of Public Service; and,
v. Selection of a sample of sectors to include for interview and document review. The selected samples include representatives from the three large science sectors 1) at the sector level for overall sector risk management, and 2) at the operational level for program risk management.

The conduct phase of this audit was substantially completed in September 2024.

Criteria

Please refer to Appendix A for the detailed audit criteria. The criteria guided the audit fieldwork and formed the basis for the overall audit conclusion.

Findings and Recommendations

Governance and Oversight

Summary finding

Overall, the Department has some established governance mechanisms to support the integration of risk management practices and principles across the Department. Senior management is well engaged in risk discussions and decisions for the development and monitoring of the Corporate Risk Profile. In addition to their current role, the governance mechanisms could be better leveraged by defining and roles and responsibilities of key players for risk management within the Department. The Department has developed a Corporate Risk Profile to articulate the strategic and operational risks faced by the Department, a draft Integrated Risk Management Framework to guide the establishment and management of the Corporate Risk Profile, and a draft Departmental Risk Management Strategy to outline the Department's approach and procedural structure for risk management. There is a need to finalize these guidance documents across the Department as tools for informed decision-making. There is also an opportunity to establish and communicate the Department's risk appetite and risk tolerance levels to inform the development of appropriate risk mitigation strategies. Finally, there is an opportunity to establish, document, and communicate a standard and consistent methodology for

the identification and assessment of risks to be used for the development of the Corporate Risk Profile (CRP) and the ongoing risk monitoring exercises, associated with the CRP.

Supporting observations

Adequate and effective governance mechanisms support the integration of risk management practices and principles across the Department. The audit assessed whether effective governance and oversight mechanisms have been established, are clearly defined, and are being properly leveraged to facilitate strategic risk discussions across all levels of the Department; whether roles, responsibilities, and accountabilities in relation to risk management are clearly defined, documented, and communicated; and whether adequate departmental guidance and strategic directives have been established within the Department to guide employees in applying risk management principles, and that this guidance is aligned with other departmental reports.

Governance and oversight

To facilitate horizontal discussion on the management of risks, the Department leverages several established governance committees, including the Senior Management Committee (SMC), the Assistant Deputy Minister Policy Committee (ADM Policy), the Assistant Deputy Minister Operations Committee (ADM Operations), the Director General Policy Committee (DG Policy), the Planning and Reporting Committee (PRC), and the Corporate Planning Network (CPN).

The Senior Management Committee (SMC) is NRCan's most senior level deliberative and decision-making committee where discussions on risk occur. SMC sets the Department's strategic directions and priorities;

oversees the horizontal planning and management of departmental activities and resources, and focuses on results achievements and risks while ensuring policy, science, program and corporate integration.

The ADM Policy Committee acts as an oversight / advisory forum that reviews departmental policy proposals to ensure consistency with the department's plans and priorities, alignment with Government of Canada direction, and integration of all sector perspectives. This committee holds joint meetings with the ADM Operations Committee on the development of risk management framework tools, such as the CRP and IBP exercise.

The DG Policy Committee supports the ADM Policy Committee by identifying horizontal policy priorities, reinforcing cross-sector policy linkages, and coordinating cross departmental policy exercises such as budgets, medium term planning and international / domestic engagement. A voting exercise was done at this committee to identify the Department's strategic and operational risks for the Corporate Risk Profile. The Planning and Reporting Committee (PRC) is a DG level advisory and decision-making body that plays on oversight role in NRCan's integrated planning and reporting process. The committee meets monthly and has representation from all sectors. It is the primary governance body with a defined mandate to provide oversight for integrated planning and reporting, including the consideration of corporate risks. The Corporate Risk Profile was endorsed at this committee before being circulated to other committees for feedback and endorsement.

The Corporate Planning Network is an informal advisory body comprised of a collaborative network of employees from various sectors and various levels, who meet monthly to provide input and feedback on proposed approaches for implementation of key corporate frameworks and share best practices for planning and reporting activities. It is the only

departmental governance body for planning and reporting that brings together sector representatives at the working level. The draft Corporate Risk Profile was presented at CPN, and feedback was sought on the risk monitoring framework.

The audit team found that these existing governance committees serve as oversight mechanisms within the Department and are being leveraged to facilitate strategic risk discussions across the Department at the DG and ADM level. The governance committees have also reviewed, provided insight, and endorsed the Department's strategic and guidance documents for risk management.

Roles and responsibilities

To effectively manage risk, organizations may develop and implement a risk management framework that defines roles and responsibilities, organizes activities, outlines resource allocations, and describes reporting and monitoring mechanisms. The audit team found that there are roles and responsibilities outlined in the following risk management strategic and guidance documents: the Corporate Risk Profile, the draft Integrated Risk Management Framework, and the draft Departmental Risk Management Strategy. The Corporate Risk Profile articulates the strategic and operational risks faced by the Department. The draft Integrated Risk Management Framework guides the development and management of the Corporate Risk Profile. The draft Departmental Risk Management Strategy aims to provide a coordinated and department-wide approach for managing risk.

All three documents outline the roles and responsibilities of the key players, including roles and responsibilities of the Deputy Minister, the primary and secondary risk leads, and all other sectors (as non-leads). The audit team found the description of the roles and responsibilities to be at the sector

level, which infers that the Assistant Deputy Minister (ADM) of that sector would ultimately be accountable. However, the documents do not provide further detail on whether specific groups/branches within the sector are responsible for monitoring the risk drivers and the implementation of risk responses. The audit team also found that there was no mention of the roles and responsibilities of managers and employees for the management of risk in their day-to-day activities.

As outlined in the draft Integrated Risk Management Framework, the Strategic Policy and Innovation Sector (SPIS) is the functional authority on risk management at NRCan. The Strategic Planning, Risk and Reporting (SPRR) Division within the Planning, Delivery and Reporting Branch of SPIS leads the development of the Department's corporate risk management strategic and guidance documents, such as the Corporate Risk Profile and the Integrated Risk Management Framework. As part of their role to support functional reviews for Treasury Board submissions and Memoranda to Cabinet, the Strategic Policy, Risk and Reporting Division also works with sectors to provide support on developing the risk sections of these documents.

Additionally, while the previously identified governance bodies play a role in risk management in the Department, including regular discussion of risk topics, and providing oversight through the review and endorsement of the Department's risk management strategic and guidance documents, the audit team found that the roles and responsibilities of the governance bodies were not identified in any of the risk management strategic and guidance documents.

The audit team also found that the documented roles and responsibilities are focused on monitoring and reporting, but do not highlight the importance of the roles and responsibilities and ownership for the

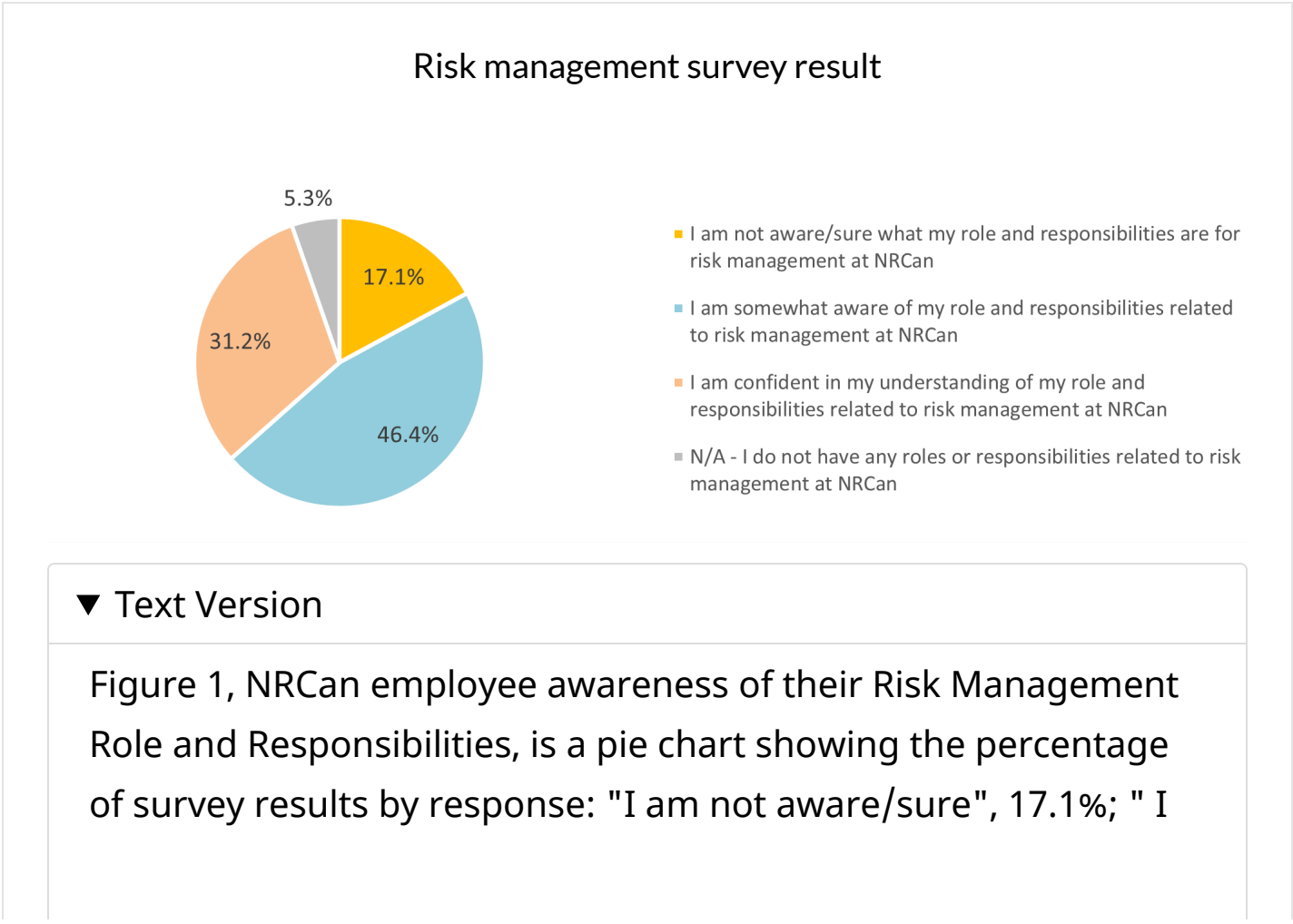
development and implementation of the risk mitigation strategies. This is especially important for risk areas that require a coordinated approach across the Department for risk mitigation. Given the decentralized nature of the Department's organizational structure, it is even more important for risk management to be well coordinated so that SPRR, risk-leads, and the appropriate functional experts in the sectors are working together to take a comprehensive approach in managing risks. For example, addressing cybersecurity risks requires the leadership of the Chief Information Officer Branch for the development of action plan items, the cooperation of sector IT personnel for the implementation of CIOB's action plan items, and the coordination of SPRR for monitoring the progress of implementing action plan items through the annual IBP cycle.

The audit team found that among risk leads and risk co-leads, roles and responsibilities were not clearly understood, beyond being responsible for coordinating with SPRR to provide updates on changes to risk drivers and implementation of risk responses. For sectors that share the responsibility for risk as co-leads, the audit team found that there was not consistent communication and coordination among the co-leads.

The TBS Framework [7] for Risk Management indicates that "a key role of the Deputy Head is to ensure that risk management principles and practices are understood and integrated into the various activities of their organization. Deputy Heads are also responsible for monitoring risk management practices in their organizations, as well as considering risks that arise when partnering with organizations within and external to the federal public service. This includes ensuring that issues affecting the organization's risk management approach, whether identified through assessments or internal and external monitoring, are examined, reviewed and addressed effectively." The audit team found that roles and responsibilities for SPIS as the Department's functional authority on risk

management is not clearly defined and understood. Based on interviews with SPIS and a review of the Department's strategic and guidance documents for risk management, the audit team found that the focus on SPRR's roles and responsibilities for risk management are mostly related to the Corporate Risk Profile and risk management at the corporate level. It does not include details of how SPRR supports the Deputy Minister in fulfilling his responsibilities for risk management as outlined in the TBS Framework. Given SPIS's position as functional reviewer with a risk lens for Cabinet documents, and their role in strategic planning and reporting, there is also an opportunity for SPIS to integrate their knowledge and expertise to inform the risk identification and risk assessment process for the CRP.

Figure 1 – NRCan employee awareness of their risk management role and responsibilities



▼ Text Version

Figure 1, NRCan employee awareness of their Risk Management Role and Responsibilities, is a pie chart showing the percentage of survey results by response: "I am not aware/sure", 17.1%; " I

am somewhat aware", 46.4%; "I am confident in my understanding", 31.2%; and "I do not have any roles or responsibilities related to risk management", 5.3%.

When asked about whether they are familiar with their role and responsibilities as they relate to risk management at NRCan, most respondents indicated that they are "somewhat aware of" (46.4%) or "confident in" (31.2%) of their role and responsibilities related to risk management. However, 22.4% of respondents indicated that they "are not aware/sure" or "do not have any roles or responsibilities related to risk management."

Although the Corporate Risk Profile and the draft Integrated Risk Management Framework are the primary tools for documenting and communicating roles and responsibilities of key players for risk management, the audit team found that these documents have not been widely communicated, which leads to a lack of awareness and clarity on the roles of responsibilities within the Department.

Strategic direction and guidance on risk management

The audit team found that the Department has established a Corporate Risk Profile and Integrated Risk Management Framework as departmental guidance intended to provide oversight and direction for the Department's risk management practices. The purpose of the Corporate Risk Profile is to "provide a concise, useable, longer-term perspective on strategic and operational risks that is integrated in organization's management practice to inform decision making, priority setting and continuous learning."

However, the audit team found that these documents do not provide sufficient guidance to employees in applying risk management principles into their day-to-day activities.

In 2022, work began for the development of the 2023-2026 Corporate Risk Profile with the discussion of risks at the Senior Management Committee Retreat, where organization risks were identified and discussed. The results of this discussion were used by SPRR to inform an environmental scan to further identify and refine the key risks faced by the Department. Insight from other departmental planning processes, such as the integrated business planning exercise, and consultations with sectors and governance committees also informed the risk identification process. SPRR identified risk leads and co-risk leads at the sector level, to be the primary and secondary parties responsible for monitoring risk drivers and implementation of risk responses and action plans, and for reporting on changes that could impact the identification, assessment, and mitigation of the risks. The risk leads and co-risk leads worked with SPRR to develop risk statements, risk drivers, and identify risk mitigation strategies. The risks were presented to three Director-General level committees (PRC, DGSTC, and DG Policy) for a voting and ranking exercise, and to determine the key risks that would be finalized in the Corporate Risk Profile. A decision was made to amalgamate several operational risks (e.g. HR, IT, real property, procurement, business continuity) into Corporate Service Delivery risk. The process resulted in six strategic risks and three operational risks being identified in the 2023-2026 Corporate Risk Profile, which was approved by the Deputy Minister in June 2023.

According to the Treasury Board Guide on Corporate Risk Profiles [8], "when developing a Corporate Risk Profile, it is important to establish a consistent methodology that clarifies how risks are aggregated from program areas to the corporate level." The audit team found that it is unclear how program

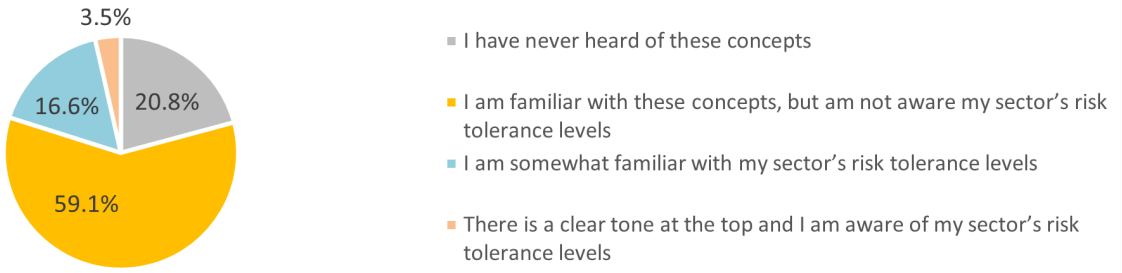
level risks are considered and aggregated when developing the Corporate Risk Profile. The templates provided to sectors for assessing the risk levels of the identified strategic and operational risks instructed sectors to provide risk ratings and mitigation for those risks as they apply to the sector. This process solicited and collected sectors' perspectives on the probability and impact of the identified risks, and their mitigation strategies for the risks as it applied to them. The audit team found that there was a lack of clarity on how sector representatives are to assess and rate the risks in a way to ensure that the risk ratings consider the perspective of the entire sector.

The audit team also found that soliciting and gathering risk mitigation strategies from the sector perspective also does not enable a coordinated approach for risk mitigation. For example, despite cybersecurity being identified as a top risk in the "high" category, the risk lead for cybersecurity noted that currently the Department has no established governance mechanism or process to assess cybersecurity risk comprehensively (sector by sector) and to aggregate the results up to the Departmental level. The audit team noted that without this comprehensive view of cybersecurity risk, the risk lead would not be able to accurately assess and validate the Department's cybersecurity risk. The voting and ranking process used to assess the strategic and operational risks consisted of having governance committee members in attendance at PRC, DGSTC, and DG Policy Committee vote on each of the risks presented, including cybersecurity, but it is unclear whether the voting sessions were preceded by branch assessments of cybersecurity risk that would be aggregated at the sector level to inform the committee members' votes. It is also unclear whether votes had the equal weight for all sector representatives, or whether larger sectors who had more representatives on the committees (e.g. more than one regional or branch representative) had more votes. The audit team

noted that CIOB is working to implement the recommendations from the recent Audit of Cybersecurity to address the areas of improvement regarding cybersecurity governance in the Department.

The Treasury Board Guide on Corporate Risk Profiles further identifies essential sections which are "considered necessary elements of a high-quality Corporate Risk Profile because they provide clarity and context." One such essential element is a Summary of Methodology, which describes "the risk assessment methodology that was used to produce the Corporate Risk Profile. In this section, organizations should provide the reader with a clear explanation of how the risk assessment was conducted and why the approach was well-suited and relevant to the organization." The audit team found that there is no clear description or explanation of the methodology used for the development of the Corporate Risk Profile. Further, none of the Department's primary risk management tools (CRP, draft Integrated Risk Management Framework, draft Departmental Risk Management Strategy) explains the process for assessing and prioritizing risks. Without having a clearly defined methodology for identifying and assessing risks (including how they are ranked and rated), and communicating the methodology across the Department, the audit team is unable to assess the extent to which a consistent and standard approach has been applied for each of the risks in the CRP, and whether the voting and ranking exercise noted earlier in the report is a suitable and relevant approach for the Department. Survey results indicate that most respondents (59%) are not aware of their sector's risk tolerance levels, and that 21% of respondents have not heard of the concept of risk tolerance.

Figure 2 – Understanding of tolerance levels in the sectors



▼ Text Version

Figure 2, Understanding of tolerance levels in the Sectors, is a pie chart showing the percentage of survey results by response: "I have never heard of these concepts"; 20.8%; "I am familiar with these concepts, but not aware of my sector's risk tolerance levels", 59.1%; "I am somewhat familiar with my sector's risk tolerance levels", 16.6%; "there is a clear tone at the top and I am aware of my sector's risk tolerance levels", 3.5%.

When asked about whether their sector conveys its [risk] tolerance levels, 20.8% of respondents indicated that they "have never heard of these concepts"; 59.1% of respondents indicated that they are "familiar with these concepts, but [are] not aware of [their] sector's risk tolerance levels; and 20.1% of respondents indicated that they are "somewhat familiar with [their] sector's risk tolerance levels" or that "there is a clear tone at the top and [they are] aware of [their] sector's risk tolerance levels."

The Treasury Board Guide on Integrated Risk Management [9] states that, "through their leadership, Deputy Heads foster a risk-informed organizational culture that supports risk-informed decision-making, enables dialogue on risk tolerance, focuses on results and enables the

consideration of both opportunity and innovation," and that "clarity on risk tolerance at all levels of the organization is necessary to support risk-informed decision-making and foster risk-informed approaches."

> "What seems to be missing in risk management is a fulsome analysis of the risk of NOT taking action on a given risk area. When we are too risk averse, we don't realize the consequences of inaction."
>
> – Response from Risk Management Survey

The audit team found that risk tolerance is discussed at various governance committee meetings. However, the Department's risk appetite and risk tolerance are not specifically defined nor communicated broadly, based on a review of information on the intranet and the Department's strategic and guidance documents for risk management. Furthermore, determining and communicating risk appetite and risk tolerance is not part of any of the roles and responsibilities outlined in these three documents, except for sectors (as non-risk leads) to communicate risk information, their approach and tolerance to risk within the sector. Without a clearly defined and communicated risk appetite and risk tolerance, it may be challenging for the Department to ensure that the identified risk responses and mitigation strategies appropriately address the risks in the CRP, and that sectors risk management activities align with the Department's risk appetite and risk tolerance.

Risk monitoring

Based on the draft Integrated Risk Management Framework, the Corporate Risk Profile is intended to be established and managed on a three-year cycle, with monitoring and reporting on a regular basis to collect updates and information to inform a Corporate Risk Dashboard. This involves SPRR

working with risk leads to collect risk data to inform updates to the risks semi-annually, and the leveraging of risk information gathered from the annual Integrated Business Planning process. The audit team observed that after the first cycle and development of the Corporate Risk Dashboard, the Department transitioned to the development and use of a Corporate Risk Snapshot instead, to report on the progress of the implementation of risk mitigation strategies.

The Corporate Risk Dashboard noted that "the ratings within the CRP were averaged with sectors input and did not present typical ratings calculated within the risk matrix formula. Therefore, with monitoring, the ratings of the risk were adjusted to best align with the proper calculation of impact and probability - which produced the variance in ratings. Risk ratings within the CRP (being averaged) presented similar levels for all 9 risks; now with monitoring a fresh perspective into risk levels from risk leads can move away from average ratings calculation to refine the inherent and residual risk levels." The audit team observed that through the Risk Monitoring Pilot, the process for assessing and rating the CRP risks have evolved. The Dashboard and subsequently the Snapshot were shared at various governance committee meetings. However, the audit team found that the Corporate Risk Profile (previous versions and current approved version), and its updates after various monitoring and validation exercises, were not broadly shared across the Department. It is not widely available on the departmental intranet (The Source), nor is it easily accessible in the Department's electronic document and records management system (GCDOCS).

Additionally, the audit team found that as the Department does not have a standard methodology for identifying and assessing risks, it is difficult to determine whether the process for validating and updating the risks during the monitoring process has the same rigour as the initial risk identification

and assessment process. It is also difficult to determine whether a consistent and standard approach has been applied for each of the risks in the CRP, and for individual sectors in their application of risk management principles to their own risk management activities. For example, the risk lead for cybersecurity noted that their involvement with the risk monitoring pilot began with a tasking to review and validate the risk rating for cybersecurity. However, there was limited explanation or instruction on the impact of the monitoring exercise. For instance, there was not a meaningful scale to align the rating to how other risks in the CRP were rated, or a standard methodology to outline how cybersecurity risks were assessed during the development of the Corporate Risk Profile to ensure that there is consistency and common understanding of how and where the rating came from. The audit team also found that the risk rating increased significantly during the risk monitoring pilot: from a rating of 7 in the Corporate Risk Profile approved in June 2023, to a rating of 16 in the Corporate Risk Snapshot presented to ADM Operations Committee in May 2024. It is unclear whether this increase is due to a changing severity of the impact and probability of cybersecurity risk events occurring, or due to a change in the process and rigour in how cybersecurity risks were assessed.

The Treasury Board Guide on Integrated Risk Management indicates that, "the corporate view of risk should be reviewed and updated regularly (potentially based on the operating context of the organization such as the annual business planning and the mid-year performance review) so that the organization always has a clear and up to date understanding of its key risks and their status to inform decision-making. If there are emerging risks that require attention in between these established cycles, an organization may wish to consider developing a mechanism that allows staff to escalate risks as appropriate." The audit team found that the Department's existing process, including the three-year cycle for managing corporate risks, does

not adequately consider the identification, assessment, and mitigation of new and emerging risks. The audit team was informed that any new risk at the Departmental level would be captured through the CRP monitoring process and would most likely fit into a previously identified risk category. This puts the burden on the initial risk identification process to define a set of risk categories that would encompass all risks that the Department could face in a three-year CRP cycle. The audit team found that outside of this categorization approach, there is no other established mechanism to identify and assess new and emerging risks, which may result in new and emerging risks that do not fit into a previously identified risk category not being properly managed. The risk mitigation strategies for the existing risks may not appropriately address the new and emerging risks.

> "The Department needs to be more aware of risks. Our approach is reactive rather than anticipatory."
>
> – Response from Risk Management Survey

The audit team noted that since the last Audit of the Integrated Risk Management Framework in 2014, the Department's approach to risk management has become less frequent, going from an annual risk management cycle to a three-year cycle, which may reduce the relevance and effectiveness of the Corporate Risk Profile as a tool to inform decision making. The audit team also noted that no previous versions of the Corporate Risk Profile are readily available to the Department. While it is outside this audit's scope to determine the rationale for the decision to modify the length of the risk management cycle since the 2014 audit, the audit team noted that combined with a lack of robust mechanism for

managing new and emerging risks, the current process may impact the Department's ability to proactively address risks in a rapidly changing environment during the three-year cycle.

The audit team noted that towards the end of the audit scope period (May 2024), SPRR had began the development of a Department Risk Management Strategy. This strategy outlines a risk update schedule that includes quarterly risk update exercises to capture new risks and anticipate the impact on established risks. It was also noted that the Corporate Risk Snapshot presented to the ADM Policy Committee in May 2024 included a discussion on actions that the Department should be taking to mitigate existing and new risks. This is a good practice and could be considered for introduction as a regular part of the Department's risk management approach.

Risk and impact

Without a process to determine and communicate the Department's risk appetite and risk tolerance, it may be challenging to establish appropriate mitigation strategies that would address the strategic and operational risks assessed. Risk mitigation strategies should be based on the Department's willingness and appetite to tolerate the impacts of risk events occurring as the Department works towards meeting its strategic objectives.

Without a robust and consistent methodology for identifying and assessing risks across the Department that aggregates and integrates risks from all levels, including new and emerging risks, there is a risk that the Corporate Risk Profile does not accurately capture and reflect all key areas of risk and their respective ratings, leaving the Department vulnerable to risk areas not previously considered and without appropriate measures to address risks arising from the changing environment in a proactive and timely manner. An inconsistent approach to measuring and monitoring risk limits

the effectiveness of the Corporate Risk Profile as a decision-making tool and hinders the Department from establishing risk mitigation strategies that align with the Department's risk tolerance and risk appetite.

Without formally and broadly communicating defined risk management roles and responsibilities across the Department, there is a risk that employees may compartmentalize risk management to certain groups or functions, and may not be aware of their responsibilities for applying risk management principles in their day-to-day activities. Without clear roles and responsibilities, there is a risk of gaps in identifying and assessing risks across the Department, as well as missed opportunities for employees to seek and obtain the support and guidance they need to apply risk management principles in their day-to-day activities. Since employees at all levels of the Department have a role to play in risk management, better clarity and more defined roles and responsibilities are needed to determine how to manage the shared responsibility for risk management across the Department.

Recommendations

Recommendation 1: It is recommended that the Assistant Deputy Minister, Strategic Policy and Innovation, strengthen integrated risk management by:

a. Reviewing the processes and documenting the methodology for developing and updating the Corporate Risk Profile. The process should clarify how risks and their ratings are identified at the corporate level, and how new and emerging risks are continually identified, assessed, and mitigated;
b. Finalizing and implementing the Department's strategic and guidance documents for corporate risk management;

c. Supporting the Department in establishing clear risk tolerance levels that are informed by the Department's overall risk appetite in collaboration with all ADMs; and
d. Clearly defining roles and responsibilities of key players for risk management, including the functional authority for risk management, ADMs, DGs, Directors, program managers, risk leads, co-leads, and governance committees.

Management response and action plan

Management agrees.

In response to Recommendation #1a:

SPI-PDR to finalize the Corporate Risk Strategy which includes the process and methodology for developing, updating, and communicating the Corporate Risk Profile (CRP). It includes a methodology for how risks and their ratings are identified and describes the process for collecting new and emerging risks. Additionally, further details on the methodology will be developed when the 2027-2030 CRP process is established.

Timeline: Q4 of 2025-26

In response to Recommendation #1b:

SPI-PDR will lead the work to update guidance documents to support corporate risk management. This includes:

a. Guidance documents for Risk-Leads and Non-Risk Leads to support the bi-annual corporate risk monitoring process. (Completed and will be refreshed yearly)
b. Corporate Risk Strategy – under development
c. Link to TBS guidance on risk management (currently in draft version of Corporate Risk Management SharePoint (Risk SharePoint) site)

The above documents will be posted on the Corporate Risk SharePoint site.

CMSS-POB will lead in establishing guidance for operational risk management under the overarching Integrated Risk Management process being established within the draft Risk Strategy. CMSS-POB manages the TBS-led Risk and Compliance Process (RCP) for NRCan, which may be leveraged in support of providing guidance on Operational Risks (TBC).

Note that while SPI has functional leadership on corporate risks, sectors are responsible for sector-level guidance and application of internal risk management approaches.

Timeline: Phased approach

- Q4 of 2024-25 - Corporate risk templates and guidance documents shared with Sector Liaison Representatives and Risk leads and non-leads via the IBP process.
- Q3 of 2025-26 – Launch of the Corporate Risk Management SharePoint
- Q4 of 2025-26 – Publication of the Corporate Risk Strategy

In response to Recommendation #1c:

SPI-PDR will work with Risk Leads to develop guidance and a structured approach for the dept to establish risk appetite and tolerance levels for the Corporate Risk Profile, as part of the next process to renew the CRP. This will be presented at governance committees (e.g., SMC) for senior management decision and DM approval. Departmental risk appetite and tolerance will be endorsed by NRCan's DM annually.

Timeline: Q2 of 2026-27.

In response to Recommendation #1d:

SPI-PDR will finalize the Corporate Risk Strategy which includes information on the roles and responsibilities of key players (e.g., SPI, Risk Leads, Non-Risk Leads, Risk Lead ADMs, DM, governance committees) for Corporate Risk Management.

SPI-PDR, in collaboration with CMSS-POB, will prepare a high-level document outlining roles and responsibilities of specific key players across the department as guidance on risk management in general (e.g., Sector ADMs, Directors, Program Managers), but would not be responsible for ensuring compliance or collecting data on outcomes. This document will be made available to all staff on the Risk SharePoint.

Note: Sector ADMs are responsible for ensuring compliance, monitoring outcomes, and clarifying sector-level roles for day-to-day risk management, and will be able to adapt this high-level document to their sector's needs.

Timeline: Q4 of 2025-26

Communication and coordination

Summary finding

Overall, the Department has established some processes and leverages existing governance mechanisms to collaborate on and coordinate the development of corporate risk management tools. There are opportunities to better communicate the Department's risk information, including the identified corporate risks and their associated risk tolerance levels and risk mitigation strategies. There are also opportunities to leverage existing Treasury Board resources and CSPS training for raising awareness, building capacity, and better equipping employees in applying risk management principles in day-to-day activities beyond the CRP exercise. Finally, there are opportunities to develop training requirements for individuals with key risk management responsibilities.

Supporting observations

Adequate and effective processes enable communication and coordination of risk management principles and activities across the Department. The audit assessed whether effective coordination mechanisms are in place between the SPIS and all sectors to enable collaboration between risk owners and the proper integration of risk considerations in the execution of departmental risk management practices on an ongoing basis. The audit also assessed whether the Department has developed adequate training activities to support employees in building their capacity to understand, implement, and integrate risk management principles into their respective roles. Additionally, the audit assessed whether effective communication mechanisms exist and are being leveraged to enable the efficient sharing of risk management information across the organization in support of timely and informed decision making.

Coordination, collaboration, and communication

> "There could be better collaboration with subject matter experts while identification, assessment, monitoring and communications of departmental level risks. Similarly, a coordinated capacity building within the department might be helpful."
>
> – Response from Risk Management Survey

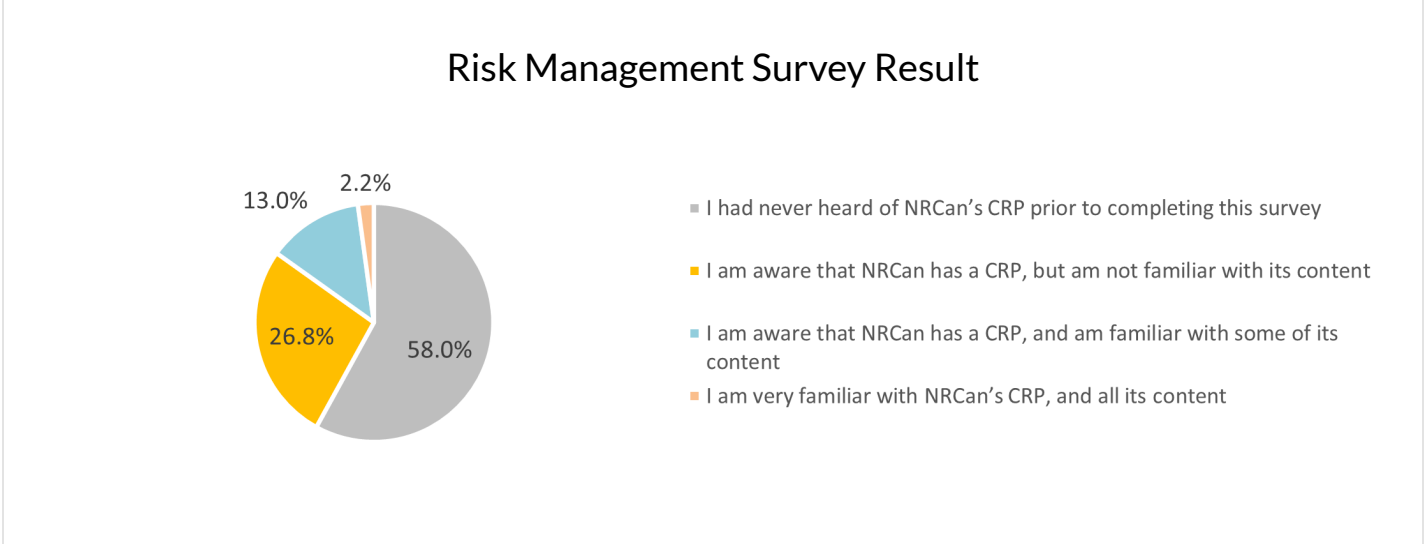
The audit team found that the current governance structure enables the facilitation of risk discussions at the management and executive levels in the Department. The governance committees mentioned in the previous section are engaged through the presentation of departmental reports and action plans, where executives discuss and provide feedback, comments and recommendations. There is also collaboration and coordination between SPRR and risk leads, and SPRR and sectors for corporate planning and reporting purposes. As part of the risk monitoring pilot, SPRR met with

identified risk leads to have risk discussions regarding the status of risk mitigation and the implementation of sector risk action plans. Through the annual IBP exercise, SPRR also engages sectors that are non-risk leads to obtain their perspectives and updates on the ratings for risks identified in the CRP.

The audit team found that there was effort put into the coordination and collaboration across the Department for the development, monitoring, and validation of the CRP. However, the results of these activities are not broadly communicated across the Department, which further limits the Corporate Risk Profile's effectiveness as a guidance tool for risk management practices.

The audit team also found that there is a lack of effective communication mechanisms to share risk management information across the Department. While the CRP exercise and subsequent monitoring pilot has been effective in generating ongoing risk discussions at the management and executive level governance committees, the audit team found that there is not an established communication mechanism for sharing risk management information across the organization in support of timely and informed decision making.

Figure 3 – NRCan corporate risk profile (CRP) awareness



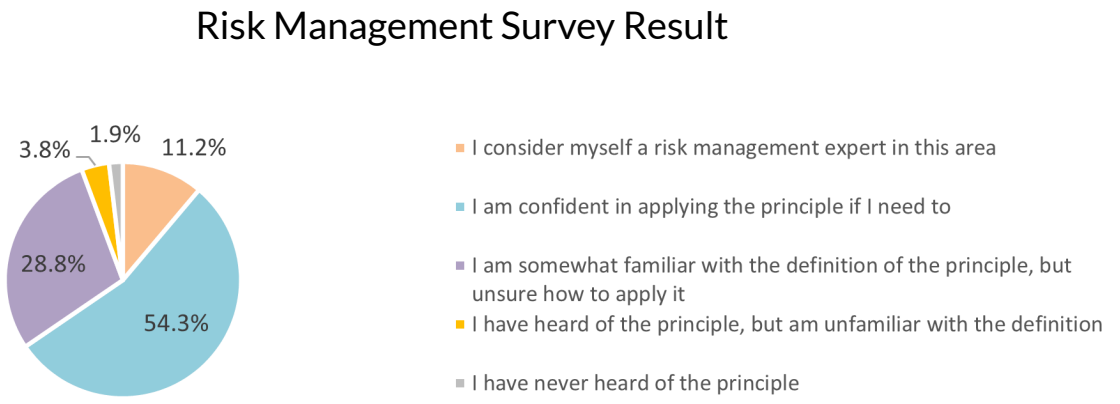
▼ Text Version

Figure 3, NRCan Corporate Risk Profile (CRP) awareness, is a pie chart showing the percentage of survey results by response: "I had never heard of NRCan's CRP prior to completing this survey", 58.0%; "I am aware that NRCan has a CRP, but am not familiar with its content", 26.8%; "I am aware that NRCan has a CRP, and am familiar with some of its content", 13.0%; "I am very familiar with NRCan's CRP, and all its content", 2.2%.

When asked about whether they are aware of NRCan's Corporate Risk Profile, 58.0% of respondents indicated that they "had never heard of NRCan's CRP prior to completing this survey", while 26.8% of respondents indicated that they are "aware that NRCan has a CRP, but [are] not familiar with its content."

Training and awareness

Figure 4 – Familiarity with risk management principles



▼ Text Version

Figure 4, Familiarity with risk management principles, is a pie chart showing the percentage of survey results by response: "I consider myself a risk management expert in this area", 11.2%; "I am confident in applying the principle if I need to", 54.3%; "I am somewhat familiar with the definition of the principle, but unsure how to apply it", 28.8%; "I have heard of the principle, but am unfamiliar with the definition", 3.8%; "I have never heard of the principle", 1.9%.

Risk management is defined as a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, making decisions on, and communicating risk issues. When asked how familiar they are with the principle, 54.3% of respondents indicated that they are "confident in applying the principle if [they] need to", while 28.8% of respondents indicated that they are "somewhat familiar with the definition of the principle, but unsure how to apply it".

As stated in the draft Integrated Risk Management Framework, one of SPRR's roles and responsibilities is to "support the improvement of the culture, capacity, and capability of risk management within the organization by providing guidance and resources on risk." SRPR developed a Risk 101 crash course, which was offered internally to employees within SPIS. The audit team found that the course materials provide high-level guidance on risk management principles and definitions relevant to the CRP exercise, which can serve as a foundation for those involved in the development of the Corporate Risk Profile and related activities. While the training may have been beneficial to employees within

SPIS, the audit noted that the examples used in the training were not tailored to a government work environment, nor specific to a scientific work environment.

In addition, the audit team found that there is a lack of information and guidance for applying risk management principles beyond the CRP exercise. The CRP and tools do not contain information and guidance to sectors on how they could be applying risk management principles to their work at all levels of the Department. Additionally, there is limited risk management guidance and information available for non-risk leads, sectors, branches, or individuals to easily leverage and to integrate risk management into their day-to-day activities. According to SPRR, they are the center of expertise for corporate risk management However, there is lack of clarity on who would be responsible for developing internal guidance for risk management unrelated to the CRP.

> "...I think NRCan needs to have a serious discussion on what risk management is, how risks are managed at different levels, and how everything ties together."
>
> – Response from Risk Management Survey
>
> Comment edited for brevity

Figure 5 – Risk management raining taken by NRCan employees

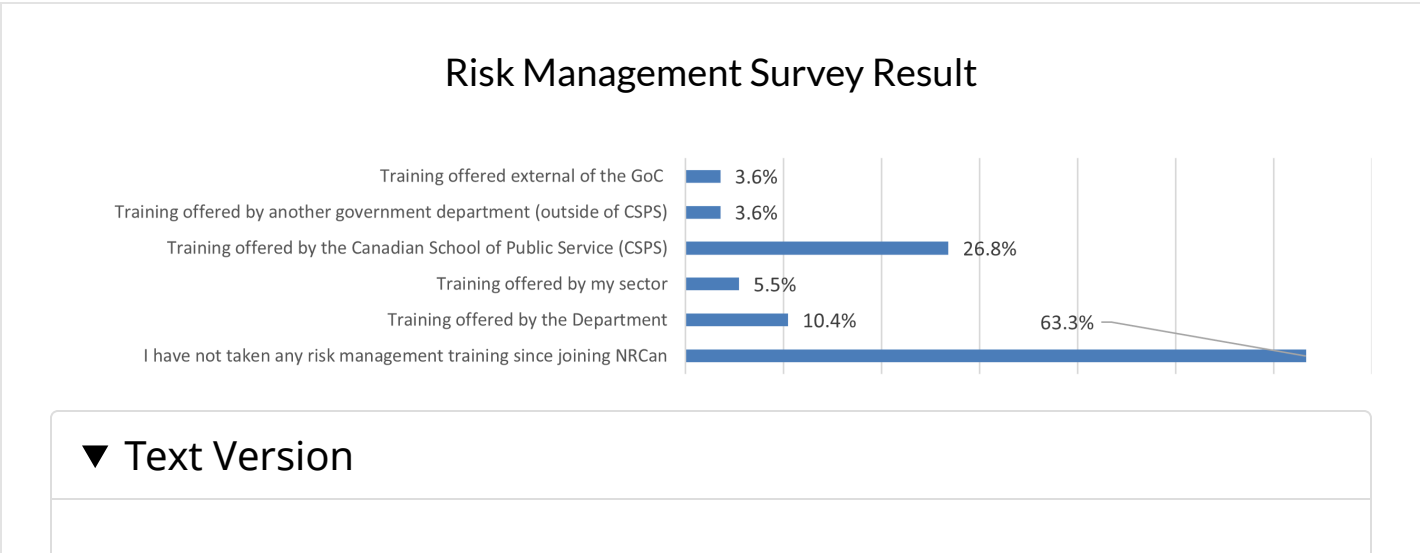


Figure 5, Risk Management Training taken by NRCan employees, is a bar chart showing the percentage of survey results by response: "training offered external of the GoC", 3.6%; "training offered by another government department (outside of CSPS)", 3.6%; "training offered by the Canada School of Public Service (CSPS)", 26.8%; "training offered by my sector", 5.5%; "training offered by the Department", 10.4%; "I have not taken any risk management training since joining NRCan", 63.3%.

When asked whether they have taken any risk management training since joining NRCan, 63.2% of respondents indicated that they "have not taken any risk management training since joining NRCan", while 26.8% of respondents indicated that they have taken "training offered by the Canadian School of Public Service".

The audit team observed that both the Treasury Board of Canada Secretariat and the Canada School of Public Service (CSPS) have guidance and training available for public servants to better understand the principles, concepts, approaches, and processes behind risk management. The primary policy instrument developed by TB is the Framework for the Management of Risk, which is supported by the Guide to Integrated Risk Management, the Guide to Corporate Risk Profiles, the Guide to Risk Statements, the Guide to Risk Taxonomies, and the Risk Management Capability Model. CSPS offers numerous courses, such as Planning Risk Management, Analyzing Risk, and Responding to Risk. Together, these two sources of guidance and training material could be leveraged to support the Department in building its capacity to understand, implement, and integrate overall risk management principles throughout the organization.

The audit team found that sector representatives interviewed (a selection of those who were responsible for risk management within their sector, and a selection of those who were responsible for programs within their sector) were familiar with and indicated that they had leveraged the Department's risk management tools, such as the 2015 Integrated Risk Management Framework and the guidance shared during the development of the Corporate Risk Profile. Of the external trainings available from CSPS, sector representatives referred to specific courses, such as the Introduction to Risk Management, and Risk Management Essentials. Some sectors identified requirements within their own teams and encouraged their staff to complete these courses as necessary.

However, the audit team also noted that numerous sectors feel that the risk information and guidance available is not applicable to their specific work. As a result, many sectors heavily rely on policies and Centres of Expertise directly related to their program or work (i.e., Grants and Contributions Centre of Expertise, NRCan Guide to Transfer Payments, etc.), rather than risk training available through internal or external means. There is an opportunity for SPRR to work with sectors to supplement or leverage the existing external guidance and training available with material that is more relevant and applicable to sector employees.

> "Employees lack the information they need to make informed decisions about many risks, such as internal risks…and external risks … Science staff are expected to just know how to manage these issues of risk management, which are outside their scientific training and expertise. More support on navigating risks/complications … is needed, so that science staff can focus on doing the science they were trained to do."
>
> – Response from Risk Management Survey
>
> Comment edited for brevity

Risk and impact:

Without effective communication mechanisms to share risk management information across the organization, there is a risk that strategic and operational decisions in the Department may not be informed by timely and relevant risk information.

Without widespread awareness and understanding of risk management principles, there is a risk that the Department will not be fully equipped to identify and mitigate risks that exist at all levels, including where and how to escalate new and emerging risks to the appropriate key players.

Without adequate training activities and guidance information on risk management principles, there is a risk that employees may not have the knowledge, understanding, and capacity to integrate risk management principles and practices into their work.

Recommendations

Recommendation 2: It is recommended that the Assistant Deputy Minister, Strategic Policy and Innovation, increase awareness and implementation of risk management principles by developing guidance, tools and training opportunities to support a strong risk management culture, through the:

a. Communication of the Department's corporate risks and the associated risk tolerances and risk mitigation strategies to all employees.
b. Development of guidance for applying risk management principles more broadly (i.e. standard methodology for identifying, assessing, addressing, and monitoring current and new and emerging risks).
c. Identification of training requirements for individuals with key risk management responsibilities.

Management response and action plan

Management agrees.

In response to Recommendation #2a:

SPI-PDR will finalize the Risk SharePoint, which will be the main hub for communicating departmental corporate risk information across NRCan. Information housed on this site will include items such as the Corporate Risk Profile (including updates to the CRP), guidance material to support the Corporate Risk monitoring process, broad high-level guidance for general risk management, and links to suggested risk resources (e.g. CSPS courses, TBS guidance). It will also include information on the Department's risk appetite and tolerance once established and approved by the DM. Additionally, governance committees will be leveraged to disseminate corporate risk information to help improve the culture throughout the department.

Timeline: Q3 2025-26 - Publication of the Corporate Risk SharePoint, with additional information added to it on an ongoing basis (e.g., risk appetites and risk tolerance once DM approved).

In response to Recommendation #2b:

SPI-PDR will finalize the Corporate Risk Strategy which provides guidance for applying risk management principles (e.g., identifying, assessing, addressing and monitoring risks). This will be shared on the Risk SharePoint site. Sectors are encouraged to leverage guidance documents to develop sector-appropriate risk practices outside the CRP, and for maintaining any risk response plans established as a condition of their policy and/or funding authorisations. Sectors will be responsible for monitoring compliance and for implementation within their respective organizations.

CMSS-POB will lead the process for developing guidance for day-to-day management of Operational Risks nested within the overarching guidance to be provided on the Risk SharePoint and taking into consideration any of the new risk requirements created by the launch of the Risk and Compliance Process.

Timeline:

Q3 2025-26 - Publication of the Corporate Risk SharePoint.

Q4 of 2025-26- Publication of the Corporate Risk Management Strategy

In response to Recommendation #2c:

SPI-PDR will identify links to CSPS courses and TBS guidance documents on risk and share this information. Sectors will be responsible for ensuring staff have taken the relevant courses to support their role in risk management.

Note: SPI-PDR provides training for risk-leads and non-leads in support of Corporate Risk Management.

CMSS-POB will establish guidance for operational risk management.

Timeline:

Q3 of 2025-26 - Training requirements to be reviewed yearly to determine if updates are required.

Risk management within the sectors

Summary finding

Overall, the audit team found that risk management principles are being applied within the sectors. The sectors vary in level of consistency and maturity in how risk management principles are operationalized in their

day-to-day activities. In the absence of departmental guidance and tools for risk management beyond the Corporate Risk Profile exercise, some sectors and branches have developed their own tools and have leveraged the available function-specific guidance for assessing risk, such as resources for transfer payment programs.

There is limited evidence of consistent and documented risk assessment exercises beyond those to meet Treasury Board submission requirements, and there is limited evidence of formalized ongoing risk management activities to identify, assess, monitor and address existing, new, and emerging risks. There are opportunities to review and consider re-establishing a requirement for sector risk profiles.

Supporting observations

Sound risk management principles, when applied within the sectors, ensures that the Department takes an integrated and holistic approach to addressing risk. The audit assessed whether effective tools and guidance are available and being leveraged by the sectors to facilitate the identification, assessment, management, and monitoring of risks within their various operations. The audit assessed whether comprehensive risk assessments are conducted during the planning stages of new programs to identify and evaluate key risk areas threatening the successful achievement of their objectives; whether measures have been established by the Programs to respond to identified risk, and whether they are being properly executed. Additionally, the audit assessed whether processes to monitor program risks have been established to re-evaluate identified risks, re-assess the appropriateness of existing risk mitigation strategies, and consider whether there are new emerging risks.

Leveraging available guidance and tools

As noted in the previous sections, there is limited risk management guidance and tools available to employees, outside of the CRP exercise. Sector employees directly involved in planning and reporting are aware of departmental guidance on CRP and related planning and reporting activities. They are actively involved in coordinating their sector's input for these exercises. Some program employees are aware of and refer to the previous (2015) version of the Integrated Risk Management Framework for risk management guidance. The sampled programs had a requirement for conducting an initial risk assessment at the onset of the program as part of the Treasury Board submission process. The audit team noted that program employees are leveraging the available information and resources specific to these types of programs, through the Department's Grants and Contributions Centre of Expertise, including risk assessment templates. Sectors are also leveraging available Departmental guidance on risk assessments for the Treasury Board submission process.

Within the sectors consulted, the audit team found that there are no specific tools and guidance developed by the sectors to guide risk management. During the scope of the 2014 Audit of the Integrated Risk Management Framework, sectors developed sector risk profiles as part of the Integrated Business Planning process. The audit team found that this is no longer being done at the sector level. The audit team also noted that the Office of Energy Efficiency (OEE) within the Energy Efficiency and Technology Sector has developed a Branch Risk Profile, guided by the TBS Framework for Risk Management and the international risk management standards (ISO 31000). It outlines the key strategic risks faced by the Branch, the existing controls in place, risk drivers, glossary of definitions, and linkages to branch- and sector-level planning products. This is

considered a best practice, and EETS and other sectors can consider adopting this practice at the sector level in the absence of available departmental guidance and tools.

Risk management practices

The audit team found that within the sampled sectors, there is more visibility and governance over sector risks where there are governance bodies put in place to discuss specific risks, such as through sector IM/IT committees, sector HR committees, and sector S&T committees. There is information flow from departmental oversight committees to sectoral committees (2 of 3 sampled sectors have established sector specific governance for these risk areas/topics). Where there are no governance bodies within the sector on these areas, information flow is not clear and is largely dependent on the sector representative to bring information back to the sector. Due to the complexity of the sector's organizational and governance structure, one sector is experiencing challenges with having visibility on sector risk management. The other two sectors have organized themselves in a way to practice integrated risk management by leveraging sector-wide governance committees. Sectors have also indicated the lack of clarity and direction on how and whether sector risk profiles should be developed and integrated with the Corporate Risk Profile.

When it comes to risk management practices within the sectors, the audit team found that all three of the sampled programs undertook risk assessments during their planning stages as part of the Treasury Board submission preparation process. Consultations were held with relevant stakeholders and subject matter experts, and the results of the risk assessments were documented in the annexes of the TB submissions.

The audit team found that there was limited documentation of risk assessment exercises beyond the initial risk assessment for the TB submission process. There is also limited evidence that programs conduct and document ongoing risk monitoring. Interviews with program representatives indicated that programs are assessing and mitigating risks as they arise, but this is not always formalized or documented. There are no formal processes in place to reevaluate identified risks, re-assess the appropriateness of existing risk mitigations strategies or address new and emerging risks.

The audit team found that measures have been established by the programs to respond to identified risks. These established measures are documented as risk response strategies within the Treasury Board submission. However, the audit team did not find formally documented rationale for selecting specific risk response strategies and rationale for why other options were not considered. This limits the understanding of the strategies' effectiveness and appropriateness. Furthermore, there is lack of clarity on how the actions will mitigate the probability or impact of risk, which can pose a challenge to assessing their potential effectiveness. The audit team also found that risk monitoring primarily occurs through adaptative management based on ongoing communication and meetings, rather than proactively identifying, assessing, and managing new and emerging risks. This approach addresses only historical and current risks and may not recognize new and evolving risks that could impact program objectives. This approach can lead to unpreparedness for future risk, increase vulnerability and result in operational disruptions and financial impacts.

Risk and impact

Without adequate and consistent guidance on how to operationalize risk management within the sectors, there is a risk that programs are not identifying, assessing, mitigating, and monitoring risks on an ongoing basis outside of the requirements for the Treasury Board submission process. There is also a risk that programs without a TB submission component are not exercising any risk management, or that risk management is done inconsistently, ad hoc, and is not supporting the program and sectors in being proactive to manage risks in a timely manner.

Recommendations

Recommendation 3: It is recommended that the Assistant Deputy Minister, Strategic Policy and Innovation, in consultation with all sector ADMs, determine whether the requirement for sector risk profiles should be re-established.

Through the implementation of audit recommendations 1 and 2, it is anticipated that the remaining findings identified in this section will be addressed.

Management response and action plan

Management agrees.

In response to Recommendation #3:

SPI-PDR will organize a discussion at SMC to determine if the requirement for sector risk profiles should be re-established.

Timeline: Q3 2025-26

Appendix A – Audit Criteria

The criteria were developed based on key controls set out in the Treasury Board of Canada’s (TB) Audit Criteria related to the Management Accountability Framework – A Tool for Internal Auditors, in conjunction with relevant TB instruments related to risk management. The criteria guided the fieldwork and formed the basis for the overall audit conclusion.

The objective of this audit was to assess whether the Department has established effective processes to ensure the implementation and integration of sound risk management principles in support of achieving its objectives.

The following audit criteria was used to conduct the audit:

Audit Sub-Objectives	Audit Criteria
Sub-objective 1: To determine whether the Department has adequate and effective governance mechanisms in place to support the integration of risk management practices and principles across the Department.	1.1 It is expected that effective governance and oversight mechanisms have been established, are clearly defined, and are being properly leveraged to facilitate strategic risk discussions across all levels of the Department.
	1.2 It is expected that roles, responsibilities, and accountabilities of the SPIS, risk leads, risk co-leads, and all departmental staff in relation to risk management are clearly defined, documented, and communicated.
	1.3 It is expected that adequate departmental guidance and strategic directives have been established within the Department to guide employees in applying risk management principles, and that this guidance is aligned with other departmental reports.

Audit Sub-Objectives	Audit Criteria
Sub-objective 2: To determine whether the Department has adequate and effective processes in place to enable communication and coordination of risk management principles and activities across the Department.	2.1 It is expected that effective coordination mechanisms are in place between the SPIS and all sectors to enable collaboration between risk owners and the proper integration of risk considerations in the execution of departmental risk management practices on an ongoing basis.
	2.2 It is expected that effective communication mechanisms exist and are being leveraged to enable the efficient sharing of risk management information across the organization in support of timely and informed decision making.
	2.3 It is expected that the Department has developed adequate training activities to support employees in building their capacity to understand, implement, and integrate risk management principles into their respective roles.

Audit Sub-Objectives	Audit Criteria
Sub-objective 3: To determine whether sound risk management principles are being effectively applied within the Sectors.	3.1 It is expected that effective tools and guidance are available and being leveraged by the Sectors to facilitate the identification, assessment, management, and monitoring of risks within their various operations.
	3.2 It is expected that comprehensive risk assessments are conducted during the planning stages of new programs to identify and evaluate key risk areas threatening the successful achievement of their objectives.
	3.3 It is expected that measures have been established by the Programs to respond to identified risk, and that they are being properly executed.
	3.4 It is expected that processes to monitor program risks have been established to re-evaluate identified risks, re-assess the appropriateness of existing risk mitigation strategies, and consider whether there are new emerging risks.

Footnotes

1 Treasury Board Framework for the Management of Risk

2 Treasury Board Guide to Integrated Risk Management

3 Canada School of Public Service’s course on Introduction to Risk Management

4 Treasury Board Framework for the Management of Risk

5 Treasury Board Guide to Integrated Risk Management

6 Canada School of Public Service’s course on Introduction to Risk Management

7 Treasury Board Framework for Risk Management

8 Treasury Board Guide to Corporate Risk Profiles

9 Treasury Board Guide to Integrated Risk Management

Date modified:
2025-05-21