NRC·CNRC

Audit of integrated risk management

Office of Audit and Evaluation

May 20, 2025

Copyright statement

The French version of this report, along with an accessible HTML version, can be found on the National Research Council of Canada's internal audit page.

This report was approved by the President of the National Research Council of Canada on May 20, 2025.

Cat. No. NR16-485/2025E-PDF
ISBN 978-0-660-77716-0

Executive summary (1 of 2)

Integrated risk management is a set of repeatable business practices, supported by a sound organizational culture, that enables an organization to assess, communicate and manage risk at a level appropriate to its risk profile, risk appetite and capacity. Integrated risk management extends beyond the assessment of risk for a specific program, business unit or objective, adopting an organization-wide perspective.

Specifically, integrated risk management enables the following:

- Risks are assessed, managed and communicated horizontally across the National Research Council of Canada (NRC), ensuring research centres, branches and the Industrial Research Assistance Program (NRC IRAP) manage risks consistently, and allow for systemic solutions to common, horizontal risks
- Risks are assessed, managed and communicated vertically at multiple levels within the organization, ensuring risks are neither over- nor under-escalated and that the most significant risks filter up to the senior-most governing body
- Risk information is incorporated into planning, oversight and decision-making processes, enabling key practices to be informed by risk considerations

Risk management should serve the broader objectives of decision making and oversight. As a leader in science, technology and innovation, tasked with addressing pressing global and Canadian challenges, the NRC must navigate a dynamic environment filled with risks and opportunities. Additionally, as a steward of public funds, the NRC must demonstrate its duty of care over government resources. Integrated risk management and risk-informed decision making are central to its ability to do so.

In a fully integrated risk management system, awareness of and responsibility for risk and risk management are distributed across the organization. While the Secretary General plays a key role in supporting the integrated risk management framework, all managers, leaders and employees bear responsibility for effectively managing the risks within their respective business units and teams they lead, as do all employees across the NRC.

What we found

We found that the NRC has established several important elements of integrated risk management that enable the organization to understand and manage its key risks. These elements include:

- a published risk management framework
- a structured process to generate meaningful risk information at the corporate level
- a culture conducive to discussing risk
- a governance structure well-positioned to oversee the risk management framework and the management of risk

However, some fundamental elements could be strengthened to fully integrate risk management across the NRC. Integration moves risk management beyond functional silos to ensure risks are managed and communicated appropriately, both vertically and horizontally, at multiple levels within the organization. Integration also requires embedding risk management into planning, oversight and decision-making processes.

We found that that although the Secretary General has developed a risk management framework that outlines an integrated approach to risk management, the framework could be improved. Specifically, it should be updated to include the full suite of roles responsible for risk management within the NRC and to detail mechanisms for integrating risk management across the organization.

Standard risk assessment processes are in place at both the corporate level and within research centres and branches. However, opportunities for improvement were identified, particularly in the monitoring of risks. Additionally, there are opportunities to better utilize risk information generated across the organization by engaging key committees, forums and other groups that possess valuable risk information.

Executive summary (2 of 2)

Furthermore, there is an opportunity to leverage the corporate risk profile for decision making by key governance committees, such as the Senior Executive Committee and the Finance, Resource and Programs Committee. We also identified the need to develop risk appetite statements to clarify acceptable levels of risk-taking, especially in areas where there are naturally differing perspectives on acceptable risk levels.

Audit opinion and conclusion

In my opinion as Chief Audit Executive, the NRC has implemented a risk management framework that establishes many of the foundational elements necessary to support the integration of risk management across the organization.

However, there are opportunities for improvement, including the following:

- Updating and implementing the risk management framework to reflect all roles involved in risk management and to provide clear guidance on vertical escalation and horizontal sharing of information
- Regularly reviewing and assessing the risk management framework to ensure its effectiveness
- Reviewing and, where necessary, improving risk management processes at both the corporate level and within research centres and branches
- Leveraging the corporate risk profile and other relevant information to inform decision making by governing bodies
- Establishing clear risk appetite statements for the NRC

Statement of conformance

This audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing and is supported by the results of the Office of Audit and Evaluation’s Quality Assurance and Improvement Program.

Introduction

Objective

To determine whether the NRC has implemented a risk management framework that is integrated [1] and supports effective decision making and oversight.

Scope

The audit examined the design and implementation of the NRC's risk management framework, with a primary focus on the role and support provided by the Secretary General, particularly the Performance Measurement and Accountability Reporting team. The audit examined the implementation of risk management at the corporate level and it also examined the risk management processes on a judgmental sample of 3 research centres and 2 branches.

The audit covered the period of April 1, 2022 to July 31, 2024. It did not examine fraud risk management or risk management activities at the program or project level. Additionally, the audit did not assess the merits of identified risks, risk ratings or risk mitigation strategies.

Approach

The audit was conducted in accordance with the Government of Canada's Policy on Internal Audit. This policy requires the examination of sufficient and appropriate evidence, as well as the collection of sufficient information and explanations to provide a reasonable level of assurance in support of the audit conclusion.

The audit approach included:

- conducting interviews and focus groups with management and key stakeholders within research centres and branches
- reviewing documentation obtained from the Secretary General, research centres and branches as well as Government of Canada guidance and best practice on risk management

[1] Shared understanding of and common behaviours in managing risk, as well as mechanisms to ensure risk information is considered and used at the appropriate levels.

The NRC’s risk management framework (1 of 3)

Context

An organization should establish and clearly articulate its commitment to integrated risk management through a policy or similar document. This provides the foundation for embedding risk management within the organization’s structures and processes.

What we expected to find

As the NRC’s foremost document on risk management, we expected to find an up-to-date risk management framework to assert the organization’s commitment to integrated risk management. Furthermore, we expected the framework would:

- outline risk management roles, responsibilities and accountabilities
- describe how risk management would be integrated across the organization, including how it would inform decision-making processes
- include clear risk appetite statements
- define mechanisms for aggregating and escalating risks
- provide a methodology to measure the performance of risk management activities

Key findings

The NRC has established a risk management framework that requires updating to reflect all roles and responsibilities for risk management at the NRC

In 2016, the NRC revised its risk management framework that committed the organization to an integrated risk management approach. The framework outlines the responsibilities of key roles for risk management, including those of the President, the Senior Executive Committee, managers and employees, the Performance Measurement and Accountability Reporting team, the Departmental Audit Committee and the Chief Audit Executive. The framework also specifies its intended outcome of navigating uncertainty more effectively to strike an appropriate balance between stewardship and innovation. The framework also reflects senior leadership’s commitment to integrated risk management and to allocating resources for its implementation.

Guided by the Institute of Internal Auditors’ (IIA) Three Lines of Defense Model, the audit team observed that the NRC has several functions comprising the second line of defense, which bear specific operational risk management responsibilities that are not currently reflected in the framework. These include the Chief Information Officer and the Executive Director of Health, Safety and Environment, who are owners of operational risk.

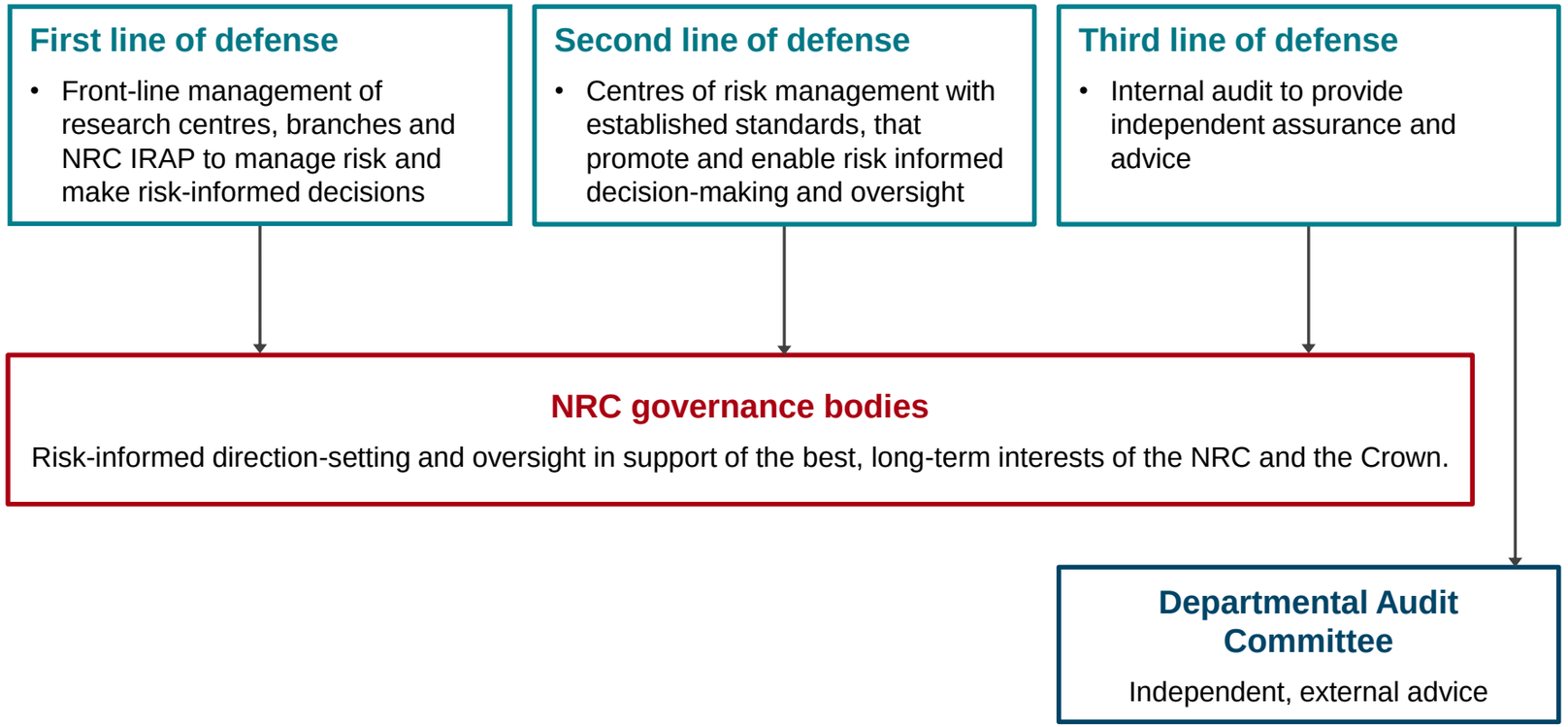
Furthermore, new governance bodies, such as the Finance, Resource and Programs Committee, have been established since the framework was last updated. These bodies complement the role of the Senior Executive Committee, which retains ultimate accountability for risk management, risk oversight and decision making. However, the roles of these new bodies are not included in the current framework. The framework also lacks guidance on how stakeholders within the risk management system should coordinate their actions and share information. In accordance with the Three Lines of Defense Model:

- the first line of defense is responsible for managing risks and establishing controls that align with the organization’s risk appetite
- the second line of defense is responsible for establishing practices for managing corporate and operational risks, for providing support to the first line, and for sharing risk information with governance bodies to support oversight and decision making

To ensure alignment across all roles, responsibilities, accountabilities and authorities, the framework should be updated to define these relationships and establish mechanisms for coordination and information-sharing. A coordinated approach, will ensure that risk information gathered and managed by the first and second lines of defense flows effectively to support oversight and decision making, enabling all functions to better accomplish their roles.

The NRC’s risk management framework (2 of 3)

Figure 1. The Institute of Internal Auditor’s Three Lines of Defense Model [2] aligned with the NRC environment



[2] Although the Institute of Internal Auditor's modified its model to the “Three Lines Model”, we felt it more appropriate to use the older term “Three Lines of Defense Model,” as it is more relevant to this audit and to effectively illustrate how the NRC is structured to defend against risk.

The NRC’s risk management framework (3 of 3)

Dimensions of risk integration

1. **Horizontal integration** occurs when risks are assessed, managed and communicated across the NRC. This provides confidence that research centres, branches and NRC IRAP manage risks consistently, enabling systemic solutions to address common, horizontal risks.

2. **Vertical integration** occurs when risks are assessed, managed and communicated at multiple levels within the organization. This approach provides confidence that risks are neither over- nor under-escalated, and that the most significant risks are appropriately escalated to the senior-most governing body.

3. **Integration of business practices** occurs when risk management and risk-related information are incorporated into planning, oversight and decision-making processes. This ensures that key practices across the organization are informed by risk.

The NRC’s risk management framework highlights many important elements for integrated risk management but could be further strengthened

The Treasury Board of Canada Secretariat’s Guide for Integrated Risk Management and the International Organization for Standardization Risk management guidelines (ISO 31000:2018) outline several provisions that should form part of a risk management policy document, such as the NRC’s risk management framework. The framework incorporates many of these provisions, including senior leadership’s commitment to integrated risk management, a requirement to review and update the risk management approach and an outline of the risk management process.

Notably, the framework describes how risk management should be integrated across the organization, emphasizing the importance of sharing information. It refers specifically to the use of a common risk lexicon (also known as a risk taxonomy) to facilitate the identification of common risk themes and ensure coherence in risk responses across multiple units, which is critical for achieving horizontal integration. However, the framework does not include all risk management roles or explain how they should coordinate to share information.

The framework addresses vertical integration by highlighting the importance of managing risks at all organizational levels while ensuring ongoing information sharing to identify interrelationships and share strategies. It emphasizes the systematic identification and escalation of risks, stating that risks rated as “high” and “very high” should be escalated. While this is a solid foundation for vertical integration, protocols for escalation should also address risks that cannot be mitigated at the lower levels or those with systemic impacts requiring intervention from the higher levels. Throughout the framework, there are multiple references to incorporating risk information and risk management into business practices. It highlights decision making and the achievement of objectives as the primary purposes of integrated risk management, emphasizing its value to the NRC’s most senior governing body.

The framework also underscores the importance of clarity on risk tolerance at all organizational levels to facilitate decision making under conditions of uncertainty. However, while the framework uses the term “risk tolerance,” it effectively describes risk appetite, risk type and the amount of risk the organization is willing to accept in pursuit of its objectives. Despite this emphasis, no formal risk appetite statements are included in the framework. These statements should be explicitly outlined to provide clear guidance.

Conclusion

The NRC has a risk management framework in place that outlines an integrated approach to risk management and includes several key provisions, such as senior management’s commitment to integrated risk management and the use of risk information to inform decision making. However, the framework could be strengthened by updating it to include the full suite of roles responsible for risk management within the NRC, incorporating detailed mechanisms to integrate risk management across the organization, and clearly outlining risk appetite statements.

Risk management processes (1 of 3)

Context

Risk management processes are essential for operationalizing risk management within an organization. Once defined, these processes enable formal risk assessments to be conducted, which can be embedded into existing structures and processes to support risk-informed decision making.

What we expected to find

We expected to find well-established risk management processes at the corporate level, and the research centres and branches, that aligned with best practices. Additionally, we expected to find guidance for risk management processes that facilitate risk-based decision making.

Key findings

Corporate-level risk management processes are defined, repeatable and generated meaningful information

A corporate risk profile standard operating procedure guides the development of the corporate risk profile. The corporate risk profile serves as an inventory of all identified corporate risks, detailing assigned risk owners, risk ratings, risk responses, mitigation measures and updates on those mitigation measures. We found that the development and maintenance of the corporate risk profile follows a standardized risk assessment process. Risks rated at 12 or higher on a 20-point scale are flagged for additional scrutiny by the Senior Executive Committee.

Although the framework emphasizes the importance of a risk lexicon to promote consistent understanding, communication and effective responses to risks, the standard operating procedure does not contain one.

The development of the corporate risk profile involves yearly environmental scanning to identify changes in the NRC's internal and external operating environments, such as geopolitical risks. Yearly consultations with risk owners, representing various areas across the organization (e.g., health and safety, finance and security), are required to assess whether risk ratings need adjustment or if risks remain relevant. These consultations contribute to horizontal integration by fostering a shared understanding of risks across different domains.

To ensure the organization's top risks are accurately identified, under the direction of the Secretary General, the Performance Measurement and Accountability Reporting team aggregates the highest-rated risks identified by research centres, branches and NRC IRAP for comparison against the corporate risk profile. This process contributes to vertical integration by ensuring that significant risks identified at lower levels are reflected in the corporate risk profile.

On a quarterly basis, risk owners of highly rated risks are consulted to provide updates, and the corporate risk profile is presented to the Senior Executive Committee for discussion. As of September 2022, quarterly updates on the corporate risk profile were consistently provided at the Senior Executive Committee meetings. Some members noted that these updates generated meaningful conversations about risk. In May 2022, the Performance Measurement and Accountability Reporting team undertook efforts to improve the corporate risk profile process. This included consultations with other government departments, which led to refinements and the introduction of an "evergreen risk profile." This approach enables dynamic, in-year monitoring of risks, streamlines senior management engagement and increases awareness of external threats.

Risk management processes (2 of 3)

However, we found that there were some opportunities for improvement. The Senior Executive Committee's terms of reference state that one of its key responsibilities is the annual approval of the corporate risk profile. This process, however, had only occurred for the 2022-2023 fiscal year. The annual approval process provides an opportunity for a comprehensive review and a challenge function, making its consistent implementation essential.

We found that, while the Performance Measurement and Accountability Reporting team tracks performance indicators in many related areas, key risk indicators had not been developed for the majority of risks, including those related to environmental impact, supply chain management and facility management. Key risk indicators provide objective information about whether risks are increasing, decreasing or remaining stable. They also complement risk owners' assessments during quarterly updates, and help assess the effectiveness of risk responses in moving risks towards acceptable levels. Ongoing and consistent monitoring of risks is essential to ensure that risk information remains relevant and up to date. This is critical for supporting decision making.

Selected research centres and branches have good risk management practices but could improve their monitoring and require strengthened guidance

A judgemental sample of 3 research centres and 2 branches was selected to assess their risk management practices. We found that a standard risk management process was in place across all 5 research centres and branches for the identification and assessment of risk, and the development of mitigation measures. This process was made mandatory through the NRC's strategic and operational planning requirements, with guidance provided by the Performance Measurement and Accountability Reporting team.

However, we found that the available guidance for research centres, branches and NRC IRAP does not include a risk lexicon, despite its inclusion in the framework as a tool to facilitate consistency in identifying and communicating risks across the organization. A common risk lexicon adopted by all research centres and branches could also simplify the Performance Measurement and Accountability Reporting team's aggregation process.

We also found that the available guidance and tools for research centres, branches and NRC IRAP could be further strengthened in the areas of monitoring, establishing risk tolerance thresholds, use of risk information for decision making and the communication and reporting of risks. The guidance often states the importance of these practices but does not provide further information on how to operationalize them. Furthermore, opportunities could be created for the research centres, branches and NRC IRAP to exchange best practices and tools.

We found less consistency in the risk monitoring practices of the sampled research centres and branches. While one research centre has developed, in consultation with the Performance Measurement and Accountability Reporting team, a management dashboard to monitor their risks over time, the other research centres and branches lack formal methods to monitor risks identified in their operational plans.

Despite this, various tools were used to track risks on a day-to-day basis. For instance, 2 of the sampled research centres leverage data visualization software, such as Microsoft Power BI, to monitor areas related to health and safety, salaries and pipeline development. These represent good practices for dynamic risk tracking. There is however an opportunity to strengthen longer term monitoring of identified risks in their operational plans.

None of the sampled research centres and branches have established thresholds for escalating risks, as risk escalation is at the discretion of the director general. However, only 1 of the sampled entities has set a risk tolerance level that would trigger more stringent mitigation measures to lower risk. Furthermore, although there is no formal guidance for research centres and branches to communicate, report on and escalate risks, good practices exist, such as team meetings, bilateral consultations between the directors general and vice-presidents, and monthly reporting templates to vice-presidents. This supports risk-based decision making.

While these practices indicate a proactive approach to risk management, there are opportunities for research centres and branches to improve their monitoring and to establish risk tolerance thresholds. There is also an opportunity to strengthen guidance and provide tools to support risk management practices in the areas of monitoring, setting risk tolerance thresholds, use of risk information for decision making and the communication and reporting on risks.

Risk management processes (3 of 3)

Conclusion

The risk management process at the corporate level is well defined, repeatable and generates meaningful risk information that is regularly discussed by senior management. However, there are opportunities to improve the process by ensuring consistent annual approvals of the corporate risk profile and developing key risk indicators.

The sampled research centres and branches demonstrate a variety of good risk management practices that support informed decision making. However, there are areas where the risk assessment process could be further strengthened. These include:

- providing enhanced guidance and tools for various risk management processes including monitoring, setting risk tolerance thresholds, escalation of risk, use of risk information for decision making and the communication and reporting on risks
- monitoring of risks identified in the operational plan and their mitigation measures
- establishing risk tolerance thresholds

Integration and oversight of risk information (1 of 4)

Context

The integration of risk is a multi-faceted process that involves horizontal and vertical integration. This means risks are assessed, managed and communicated across the organization, and at multiple levels. Integration also requires that risk management and risk information be embedded into planning, oversight and decision-making processes.

Governing bodies play a critical role in integrated risk management by ensuring a robust risk management system is in place and is functioning effectively.

What we expected to find

We expected to find explicit processes designed to facilitate both the horizontal and vertical integration of risk management across the NRC. Additionally, we anticipated processes to promote the use of risk information in decision making.

We also expected the Senior Executive Committee to oversee the implementation of the NRC's risk management framework.

Key findings

The Senior Executive Committee contributes to the management of risks through consistent oversight of the corporate risk profile, however there is an opportunity to strengthen the Senior Executive Committee's role in risk management

The Senior Executive Committee regularly reviews the corporate risk profile on a quarterly basis and oversees critical risk management issues as they arise. For instance, projects with significant risk levels, such as those managed by the Office of Facilities and Renewal Management, attend Senior Executive Committee meetings regularly to provide status updates. In this capacity, the committee is instrumental in overseeing the management of risks identified in the corporate risk profile.

However, we noted that there are opportunities for the Senior Executive Committee to take a more active role in overseeing and monitoring the overall risk management framework, its application and the effectiveness of the NRC's risk management approach.

The framework outlines requirements for both the Performance Measurement and Accountability Reporting team and the Senior Executive Committee to engage in ongoing monitoring and periodic reviews of the framework. It also includes performance measures to assess whether the organization's risk management approach is successful. Currently, the Performance Measurement and Accountability Reporting team's assessments focus solely on the process of developing and maintaining the corporate risk profile. While this ensures the effectiveness of the corporate risk profile, there is also value in ensuring that risk management is effectively implemented across the organization to support management's objectives.

A regular review of the appropriateness and usefulness of the framework could add significant value by fostering continuous improvement and accountability in risk management. This review could take the form of a self-assessment, during which the Performance Measurement and Accountability Reporting team and Senior Executive Committee could reflect on the following questions:

- Are the NRC's objectives for risk management still current and relevant in the context of the internal and external environment?
- Are the roles and accountabilities clear, relevant and well understood, including those of governance bodies?
- Are the risk management processes that are in use across the NRC efficient, effective and generate meaningful and actionable information?
- Is the NRC's risk appetite clear and relevant, given its objectives, risk profile and capacity for risk mitigation?

Integration and oversight of risk information (2 of 4)

The corporate risk profile contains valuable information but is underutilized in decision making

The NRC has an established governance and oversight structure in place. In addition to the Senior Executive Committee, the organization's primary internal decision-making body, the Finance, Resource and Programs Committee was formed in 2023 to provide greater scrutiny over the organization's use of resources. That same year, the NRC also created the Safety Operations Committee, a subcommittee reporting to the Senior Executive Committee, with a specific focus on health and safety risks. These developments demonstrate the organization's commitment to strengthening governance over risk management.

However, we found that some governing bodies do not consistently use corporate or other risk information to inform their deliberations and decision making. While the corporate risk profile is reviewed by the Senior Executive Committee, the information it contains is not formally used as an input for decision making or oversight. Furthermore, no formal process exists to ensure the corporate risk profile is referenced in requests for decisions about resources or strategies.

We reviewed a judgemental sample of minutes from Senior Executive Committee and Finance, Resource and Programs Committee meetings and found that although risks related to specific projects or initiatives were often discussed, the corporate risk profile was not explicitly considered in decision making or in requests for resources.

The effect of not explicitly using the corporate risk profile in decision making is two-fold:

- It results in missed opportunities for more informed oversight and decision making
- It makes it more challenging to demonstrate the value of risk management as a meaningful management tool

Some feedback was received on the perceived limited use of risk information collected as part of corporate risk profile and operational planning processes. This presents an opportunity to better leverage this process to strengthen integrated risk management and informed decision making. Explicitly incorporating the corporate risk profile and operational risk information into governance discussions and decision-making processes would strengthen the perceived and actual value of risk management and therefore its uptake.

The corporate risk profile and related reports provide valuable insights into the NRC's priorities for risk mitigation. Leveraging this information can help align resources with these priorities, and enhance the resilience and responsiveness of operations.

Integration and oversight of risk information (3 of 4)

Clearer roles and protocols are needed to strengthen the Performance Measurement and Accountability Reporting team's role as an integrator of risk management

The framework assigns the Performance Measurement and Accountability Reporting team the responsibility of supporting the organization in implementing the NRC's risk management framework. The team leads the corporate risk profile process, while research centres, branches and NRC IRAP are responsible for risk management at the operational level. Additionally, the Performance Measurement and Accountability Reporting team provides guidance, tools and further support when requested.

While the team has contributed toward aligning specific risk management functions and integrating them into key business processes, we found that there were opportunities to enhance the integration of risk information and clarify accountabilities and expectations for sharing this information.

The annual and quarterly updates on the corporate risk profile, along with the Performance Measurement and Accountability Reporting team's aggregation process, contribute to integration across the organization. Yet, the current aggregation process is conducted only once a year, leaving emerging risks that arise throughout the year unaccounted for. Additionally, the process does not take into consideration lower-rated but pervasive risks that might warrant corporate-level attention. The annual and quarterly corporate risk profile updates are largely informed by senior executive leaders and do not incorporate insights from lower levels of the organization.

A more data-informed approach to collecting and utilizing operational risk information across the NRC could strengthen integration. Tools such as an assurance and oversight map, which identifies existing data sources and their owners, could supplement the corporate risk profile and reinforce both the repeatability of the process and the roles of other parties in the risk management cycle.

Reliance on objective data from existing sources, such as key performance indicators, the Public Service Employee Survey and data from the NRC's hazardous occurrence report system, could further inform the quarterly and annual updates.

The Performance Measurement and Accountability Reporting team currently has less frequent risk-focused engagement with other parts of the organization where risk information resides. Committees and forums such as the Executive Committee, Directors General and Executive Directors Committee, Management Community, communities of practice and groups of cohorts (such as directors of operations) hold significant knowledge about risks within the NRC. However, this risk intelligence is not systematically mined to inform the corporate risk profile and to enhance management's oversight of risks.

While the Performance Measurement and Accountability Reporting team has delivered some operational planning presentations that provide information about the risk assessment process, there has been limited engagement otherwise and there is an opportunity for the Performance Measurement and Accountability Reporting team to better leverage these groups to consult them on risks and risk management practices at the NRC. Without these connection points built into the risk management system, there is no assurance that all risks warranting escalation have been identified or that pervasive issues requiring collective resolution are being addressed.

For instance, we found, through interviews and a review of operational plans, that 7 research centres and branches are actively seeking or have implemented solutions to consolidate health and safety program information, including assessments and training records. Proper logging of this information facilitates the management of health and safety programs, which serve as mitigation measures against work place incidents. Similarly, conflicting notions of risk appetite across groups that collaborate to advance the NRC's objectives present challenges to effective risk mitigation.

To address these gaps, it is important to further define the role of the Performance Measurement and Accountability Reporting team as the integrator of risk management. This includes clarifying the sources of information the team should rely upon to identify risks warranting escalation and issues requiring support or resolution. Establishing multiple connection points within the organization would keep the Performance Measurement and Accountability Reporting team informed of risk management issues across all levels and ensure that information flows appropriately to facilitate resolution and enhance support for risk management efforts.

Integration and oversight of risk information (4 of 4)

Conclusion

The NRC has established processes to support governance, decision making and oversight. However, there are opportunities for the Senior Executive Committee to take a more active role in overseeing and monitoring the overall risk management framework and assessing whether the NRC's risk management approach has been effectively implemented across all levels.

Additionally, strengthening the coordination between the Performance Measurement and Accountability Reporting team, as the owner of the corporate risk profile, and other functions where risk information resides could significantly enhance the integration of risk management. Improved coordination within the risk management system would provide greater assurance that all risks warranting escalation have been identified and that pervasive issues are identified for collective resolution.

The NRC’s risk culture (1 of 2)

Context

Risk culture refers to the attitudes and behaviours associated with risk management. A healthy risk culture views risk management as integral to sound decision making and embeds strong risk management principles and practices at all organizational levels. An environment that fosters open dialogue about emerging risks, risk taking and risk tolerance supports a positive risk culture. Furthermore, risk appetite, the amount of risk an organization is willing to accept in pursuit of its objectives, should be clearly defined and understood across the organization.

What we expected to find

We expected to find evidence of a positive risk culture at the NRC, as well as clear and explicit risk appetite statements set by the senior governing body and understood by employees.

Key findings

The NRC promotes a culture that fosters open dialogue about risks

Our audit included interviews and focus groups at various organizational levels, including one-on-one interviews with vice-presidents, directors general, directors, and focus groups with directors, managers and team leads across research divisions, corporate branches and in business development. A majority of interviewees indicated that the NRC fosters an environment where employees feel comfortable discussing and raising concerns about risk.

Interviews and document analysis revealed examples of proactive risk management approaches that reflect a positive risk culture. One example was the **Take 5 minutes!** safety-at-work tool, which involves a 5-minute, 5-step personal risk assessment to encourage employee vigilance in identifying and controlling immediate risks in the workplace. This tool was recently implemented by one of the research centres we sampled. Another research centre we interviewed incorporates risk-based thinking into its technical training, covering concepts such as risk appetite, risk tolerance and the risk management process. Additionally, in 2023, the NRC undertook a climate change vulnerability study of its infrastructure portfolio. This initiative helps decision-makers prioritize efforts and investments to reduce risks and improve resilience to climate change.

Opportunity exists to define the NRC’s risk appetite for alignment and balance on risk-taking

A reoccurring theme from interviews and focus groups was the variation in risk management priorities and risk appetite across the organization. The NRC’s diverse portfolio includes stewardship and compliance with government policies as well as innovation, research and development, and commercialization. While it is appropriate to adopt a risk-averse approach for stewardship and compliance and a more risk-open approach for innovation and research, areas of overlap exist. Particularly in research centre operations where collaboration with corporate services is required to address health and safety, research security, contracting, procurement and other risks.

Interviewees from research centres described collaborative relationships with corporate services but noted challenges where decisions did not fully consider the trade-offs between mitigation measures and their impacts on the speed and cost of advancing their work. They described delays and resources constraints arising from mitigation measures they perceived as disproportionate to actual risks, such as those related to health and safety or contracting. Interviewees on the frontlines of managing corporate risks held opposing views, noting at times a disconnect between controls necessary to conduct research securely and safely, and their adherence.

The NRC’s risk culture (2 of 2)

These differences highlight the tension inherent in balancing the NRC’s objectives. Without clear guidance on risk appetite, employees may take risks that exceed the organization’s risk appetite or miss opportunities due to excessive risk aversion. This can hinder the achievement of compliance-related objectives as well as those related to research and development.

Risk management should be seen as a continuum, informing an appropriate level of mitigation rather than relying on a one-size-fits-all model. Clear risk appetite statements, aligned with the NRC’s objectives and capacity to take risks, would enable the NRC to articulate its position on the naturally differing perspectives regarding acceptable levels of risk. This would establish a clear risk acceptance and management system, ensuring the various parts of the organization are aligned on what constitutes acceptable risk. Employee decisions would then be grounded in a shared understanding of the organization’s risk appetite in any given scenario.

Conclusion

The NRC has an open and risk-aware culture where employees feel safe in communicating their concerns about risk. However, there is an opportunity to ensure balanced risk-taking and a common understanding among employees through the use of risk appetite statements. This clarity will help the NRC effectively manage risks, enabling a healthy balance between stewardship and innovation at all levels of the organization.

Recommendations (1 of 3)

Recommendation 1

The Secretary General should review and update the NRC's risk management framework to include the following:

- The full suite of the NRC's risk management roles, responsibilities, accountabilities and authorities, in alignment with the Three Lines of Defense Model.
  - This should include how these roles work together to ensure an efficient, integrated approach for risk management
  - Developing an assurance map may help identify various sources of risk intelligence that can support a "measure once, use many times" approach to risk management
- A common risk taxonomy with clear guidance on criteria for vertical escalation and horizontal sharing of information
- Clear risk appetite statements aligned with the NRC's business objectives and capacity for risk mitigation.
  - The Secretary General, in consultation with the Senior Executive Committee, should ensure the risk appetite statements are clear, relevant and reflect the organization's objectives, risk profiles and mitigation capacity.
  - This would include engagement with employees to address differing perspectives on risk appetite, clarify concerns and promote alignment on risk-taking and risk-averse behaviours that are consistent with the NRC's risk appetite

Management action plan

The Policy, Strategy and Performance Branch agrees to review and update the NRC's risk management framework, including:

- redefining the full suite of the NRC's management roles and responsibilities, and considering how an assurance map may support this process
- updating the existing risk taxonomy with appropriate guidance for vertical and horizontal escalation through forums and communities of practice to share best practices
- defining risk appetite statements aligned with the NRC's business objectives, risk profiles and mitigation capacity

Senior Executive Committee approval will be sought for the updated risk management framework.

Expected implementation date: The NRC's risk management framework will be updated and approved by the Senior Executive Committee by March 31, 2026.

Contact: The Director of the Performance Measurement and Accountability Reporting team.

Recommendations (2 of 3)

Recommendation 2

The Secretary General should review and, where necessary, strengthen the risk management processes, tools and guidance at the corporate, research centre, branch, and NRC IRAP levels. This includes:

- ensuring consistent application of the corporate risk profile process
- supporting assigned risk owners within the corporate risk profile to develop risk indicators that provide objective measures of risk, considering integration with existing performance measurement indicators
- engaging the research centre, branch and NRC IRAP levels to understand their needs and provide more comprehensive guidance and tools to address the most significant gaps to contribute to effective integrated risk management, including guidance for the following areas:
  - risk monitoring
  - setting risk tolerance and thresholds for escalating risks
  - communication and reporting of risk information
  - use of risk information in decision making

Management action plan:

The Policy, Strategy and Performance Branch will consistently support the corporate risk profile process, while recognizing opportunities to continue to improve the process and better meet the needs of the NRC.

The Policy, Strategy and Performance Branch will also work with corporate risk owners to develop risk indicators for inclusion in the corporate risk register and establish processes for their effective monitoring, which may include leveraging existing performance measurement indicators.

In addition to the updated framework described in recommendation 1, the Policy, Strategy and Performance Branch will work with other risk practitioners at the NRC to identify existing tools and develop guidance to support effective risk management at the NRC. These may include:

- identifying or establishing a forum to share best practices, guidance and new tools amongst risk practitioners
- exploring additional tools to support effective risk monitoring, management, reporting and use of risk information at other levels of the organization

Expected implementation date: The corporate risk profile is to be updated with indicators and monitoring strategies by November 30, 2025. A forum to share risk management tools between the research centre, branch and NRC IRAP levels and other risk practitioners will be identified by November 30, 2025

Contact: The Director of the Performance Measurement and Accountability Reporting team.

Recommendations (3 of 3)

Recommendation 3

The Secretary General should review relevant processes and guidance to ensure that the corporate risk profile and other risk-related inputs are leveraged by governing bodies for decision making. These inputs should also be used as sources of information when seeking endorsement or decisions from governing bodies.

Management action plan:

The Corporate Secretariat will:

- issue written guidance to the Executive Committee members on expectations related to incorporating risk-related inputs into submissions for the Senior Executive Committee, the Finance, Resource and Programs Committee and the Safety Operations Committee
- meet at least twice yearly with the Performance Measurement and Accountability Reporting team to verify that risk-related inputs continue to be effectively leveraged by the Senior Executive Committee, the Finance, Resource and Programs Committee and the Safety Operations Committee for decision making

Expected implementation date:

Written guidance to the Executive Committee members on expectations related to incorporating risk-related inputs into submissions for the Senior Executive Committee, the Finance, Resource and Programs Committee and the Safety Operations Committee will be issued by December 31, 2025. The Corporate Secretariat will ensure that meetings are held at least twice yearly with the Performance Measurement and Accountability Reporting time by December 31, 2025.

Contact:

The Executive Director of the Corporate Secretariat.

Recommendation 4

The Secretary General, in consultation with the Senior Executive Committee, should ensure that the NRC's risk management framework is regularly reviewed and assessed for effectiveness. This assessment should extend beyond the corporate risk profile process and include:

- evaluating the continued relevance of roles and responsibilities
- assessing whether risk management processes in use across the NRC are effective and result in meaningful information
- determining whether the NRC's risk appetite statements are clear and aligned with its objectives and risk profile

Management action plan:

The Policy, Strategy and Performance Branch will include expectations for the review of the NRC's risk management framework, both scope and frequency, in the updated risk management framework.

Reviews will then be conducted in alignment with the approved updated risk management framework.

Expected implementation date:

Approval of the updated framework will be received by March 30, 2026.

Contact:

The Director of the Performance Measurement and Accountability Reporting team.

Annex A: Audit criteria

1. **Governance and oversight**
   i. There is an appropriate risk management policy or framework and governance bodies and decision makers implement and adhere to the NRC's requirements for risk management, which are aligned with the Treasury Board of Canada Secretariat guidance and best practices.
   ii. Risk management roles and responsibilities are defined, communicated and complied with by stakeholders.
2. **Risk management processes**
   i. Processes, guidance and tools for integrated risk management have been established and are consistently applied at the corporate, research centre and branch and NRC IRAP levels.
3. **Monitoring, communication and use of risk information**
   i. The NRC's organizational culture is characterized by open and proactive discussions about risk, and the use of risk information to inform oversight and decision making.
   ii. The risk management system is monitored for effectiveness and compliance, in support of continued improvement.