Audit of Integrated Risk Management - Health Canada

Final Report

December 2022

Health Canada and the Public Health Agency of Canada
Santé Canada et l'Agence de la santé publique du Canada

Office of Audit and Evaluation

Executive Summary

Introduction

The effective integration of risk management into an organization's governance, structures, and programs supports department-wide decision making and key management functions, including policy development, planning and priority setting, resource allocation, and performance assessment at the departmental, branch, and program levels.

At Health Canada (HC), risk management is a shared responsibility among managers at all levels. The Departmental Submissions and Performance Measurement Directorate (DSPMD) leads the development of the Corporate Risk Profile (CRP), which identifies high-level, strategic organizational risks. In addition, each branch is responsible for developing and implementing initiatives that address the risks identified in the CRP, as well as those specific to their mandates and operations. Departmental policy frameworks include flexibility on how individual branches and business units tailor risk management activities and processes to meet their needs. This audit considered the impact of this flexibility in its assessment of the overall departmental risk management framework.

The Treasury Board of Canada Secretariat's (TBS) Framework for the Management of Risk (2010) provides broad risk management principles and sets out expectations for deputy heads and their departments. The TBS Guide to Integrated Risk Management (2014) builds on the principles of the Framework and provides guidance on the design, implementation, conduct, and continuous improvement of integrated risk management. The criteria used to assess the Department's risk management framework and practices reflect risk management principles and expectations of the associated TBS Framework and Guide. They are also linked to international risk management standards, as outlined in the International Organization for Standardization (ISO 31000) Risk Management Principles and Guidelines, and the Committee of Sponsoring Organizations (COSO)'s Enterprise Risk Management (ERM) Framework.

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.

Engagement Objective

The objective of the audit was to assess whether the Department's risk management framework and practices effectively support the identification, assessment, and integration of risk information for planning, oversight, and decision-making purposes.

Engagement Scope

The audit scope focused on risk management processes and activities at the corporate and branch levels, from April 1, 2019 to Dec 31, 2021. The audit examined policies and governance frameworks, roles and responsibilities. And processes, tools, and procedures to identify, assess, and respond to risks. The audit also examined processes for monitoring and reporting risk information, and for integrating this information into the Department's planning and reporting cycles. The scope did not include assessments of the appropriateness of the risks identified, the actual risk levels or ratings, nor the risk responses determined by management.

What We Found

HC's corporate and branch level risk management practices generally support the identification and integration of risk in planning and decision-making processes. However, there are opportunities for the Department to improve risk management at the branch level by formalizing and standardizing related practices.

HC formally identifies and assesses its strategic-level risks using the CRP. The Department has assigned responsibility to individual branches to develop and implement responses to the risks identified in the CRP. DSPMD reviews each branch's results achievement, as well as their associated risk responses on an annual basis, and incorporates them into the Departmental Results Report.

The Department's branch and directorate levels use operational planning processes to identify priorities and associated risks, and monitors progress on these initiatives and priorities through existing governance structures. However, risks are not consistently considered at senior level committees, and the Department has not defined roles and responsibilities for monitoring and reporting on risk management practices. In addition, the Department does not provide formal risk management training to its employees.

HC could improve and further strengthen risk management practices by:

- clarifying roles and responsibilities and standardizing risk management processes and tools;
- incorporating risk-specific items into senior committee agenda items for review, discussion, and endorsement;
- implementing risk management-specific training initiatives; and
- enhancing the process for ongoing risk monitoring, including the regular assessment of risk practices and the effectiveness of risk responses.

Criterion 1 - Governance

Context

Integrating risk management into governance processes supports management in delivering its mandate by facilitating faster and better informed decisions, ensuring the best allocation of resources, and ensuring compliance with policies and legislation. It also helps the Department to recognize, understand, accommodate, and capitalize on new challenges and opportunities, and to bring a strategic and comprehensive focus to addressing horizontal risks that require sustained attention.

Integrated Risk Management was removed from the Management Accountability Framework (MAF) prior to the determination of the scope of this audit. The absence of MAF assessments of integrated risk may have reduced the Department's focus on integrated risk management processes. This, combined with the volatile and resource intensive COVID-19 operating environment, may have adversely affected the level of progress and engagement on risk management policy initiatives over the last few years.

What We Expected To Find

We expected to find that appropriate governance frameworks support integrated risk management (IRM) throughout the Department, including established policies and standards, clearly defined roles and responsibilities, and appropriate bodies to provide direction and oversight.

Key Findings

Policy and Directives

The Department has drafted a HC Risk Management Policy (the Policy) and accompanying Risk Management Guide (the Guide), which are aligned with the TBS *Framework for the Management of Risk* (the Framework) and the TBS *Guide to Integrated Risk Management.* Together, they outline key elements of risk management, including objectives, guiding principles, roles and responsibilities, risk management concepts, and key steps of the risk management life cycle. However, the Policy has been in draft form since early 2021 and has not yet been presented to senior management for approval.

Though the expected results of the Policy include common approaches and greater consistency in risk-based decision making across the Department, the Policy does not identify common baseline expectations for all branches regarding risk management processes and deliverables. Defining and communicating these expectations would support each branch's risk management processes and the Policy's objective of enabling common approaches and greater consistency of practice. It would also facilitate oversight and assessment of the Policy and Framework's implementation, and streamline the Department's efforts to consolidate and integrate risk information that is critical for the development of the CRP.

Roles and Responsibilities

The Department has outlined risk management roles and responsibilities in the Policy, including those for key governance bodies. However, it does not assign a functional authority responsible for monitoring risk management and compliance with the Policy and standards. CFOB officials stated that their risk management focus is limited to the CRP process. A clearly defined functional authority would better support the Deputy Head in monitoring and assessing the integration of risk management practices across the Department.

Although the Policy does not define roles and responsibilities for managers at the branch level, the audit found that management generally understood risk management principles and considered risk in their plans and activities. Terms of reference for branch-level governance bodies also include general expectations and guidance on risk management.

Governance Bodies

The terms of reference (TOR) for senior management committees at the departmental level, and within branches, include responsibilities for providing leadership, direction, and oversight for key management functions, including risk management. At the Branch Executive Committees (BECs) and directorate-level committees, risk discussions take place through ad hoc presentations by the branch's planning and reporting units, and through presentations by DGs or Directors on their plans, priorities, and associated risks.

The Executive Committee (EC)[1] is supported by sub-committees that serve as forums for discussion, review, and escalation of risk issues within their respective mandates. However, items explicitly addressing risk management are not formally integrated as standing items on senior committee agendas. There is no evidence of EC discussions related to the CRP, nor its annual review and endorsement. Departmental Audit Committee (DAC) members were engaged secretarially to provide input on the 2019-22 CRP, but reviews of the CRP and the departmental risk management structure were not included on DAC meeting agendas during the audit period. The absence of formal risk management discussions at senior management governance body meetings reduces senior-level oversight, engagement, and endorsement of risk management practices in the Department.

[1]The EC is the most senior direction-setting, decision-making, and oversight body.

Conclusion

The draft departmental Policy and related governance processes provide some guidance and structure for risk management practices; however, they do not adequately support and maximize the benefits of IRM throughout the Department. The Policy and governance structures would benefit from:

- clearly defined roles and responsibilities for CFOB as the functional authority over risk management;
- baseline expectations for branch-level risk management processes; and
- integration of formal and regular risk management oversight activities at senior committees, including the EC and the DAC.

Recommendation #1:

The CFO should ensure that the new Risk Management Policy and related Guide:

- Clearly establish minimum expectations for branches regarding risk processes and associated risk management outputs;
- Establish and clarify the roles and responsibilities of CFOB with respect to functional authority over risk management practices across the Department, including monitoring, assessment, and reporting on practices and compliance with HC's Risk Management Policy;
- Define a process for a periodic review, assessment, and reporting on the status of HC risk management practices; and
- Ensure that risk management updates, including the results of CRP annual reviews, are incorporated as standing items on EC and DAC agendas on a regular basis.

Criterion 2 – Risk Management Processes

Context

Integrated Risk Management supports a continuous, proactive, and systematic approach to managing risk from an organization-wide perspective. Having consistent processes for managing risks throughout the organization helps with aggregating risk information at the corporate level to better address challenges facing the organization.

This requires ongoing assessments at every level of the organization, and the capacity to aggregate and communicate their results in a cohesive and consistent manner.

Formalization and standardization of risk management practices across the Department would enhance the ability to systemically integrate risk information for senior management's consideration and decision making. This would in turn facilitate the monitoring and implementation of risk management processes in the Department.

What we expected to find

We expected to find that risk management at all levels is supported by established processes, guidance, and tools.

Key Findings

The CRP is the key departmental IRM tool used to identify strategic risks at the corporate level that could affect the achievement of the Department's mandate. It identifies risks in three-year cycles, with a requirement for annual reviews and updates. The CRP provides a framework for conducting the CRP exercise, provides context and rationale for risks, identifies strategies to mitigate them, and assigns branches as leads to plan mitigation measures for individual risks. The framework includes guidance on how to conduct the CRP exercise, as well as the requirements for monitoring risks and risk responses. Although senior management committees have not reviewed nor endorsed the 2019 to 2022 CRPs, an annual review and update of risk responses is being conducted through the Departmental Planning (DP) and Departmental Results Reporting (DRR) processes. DSPMD circulates the previous year's CRP and asks senior branch level managers to identify new risks for consideration in the CRP update. We note that, with the exception of a sixth risk associated with the COVID-19 pandemic that was proposed by the Departmental Audit Committee, the CRP risks have remained relatively unchanged since the prior three-year CRP cycle.

At the branch level, risk management practices are generally included in operational planning and reporting processes. Interviewees indicated that risk management is informally considered part of regular and ongoing bilateral or multilateral meetings among DGs, directors, and managers. The audit team reviewed a sample of branch and directorate operational plans and found that priorities and associated risks were identified through the planning processes. However, operational plans varied in format and content. For example, some plans were consolidated and presented at the branch level and, in other instances, individual directorate plans were used as tools for considering risk. Some branch plans were directly linked to the CRP or other identified risks, while others did not link priorities or risks to the CRP. Individual directorates within branches have developed or are developing their own templates for operational plans that are intended to more effectively demonstrate how priorities are linked to risks and how risk is considered in planning processes.

Although risks are considered in operational planning and reporting processes, there was little evidence of formal, systematic branch-level risk frameworks or processes to identify risks, to assign risk levels and risk responses, nor to monitor risks (e.g., use of templates, risk registers, risk scales, 'heat maps', risk tolerance matrices). It is not clear why branch risk registers were no longer required and were not consistently developed nor maintained. In cases where branch risks were identified, they primarily reflected the CRP risks with little additional context or information. We noted that some branches have been undertaking risk-management improvement initiatives, such as developing their own, more formalized, risk management frameworks and processes.

The Department does not currently offer formal training on risk management and online guidance is limited. Interviewees indicated that risk management is intuitively and implicitly practiced on a daily basis, and consideration of risk drives all decisions. Despite this, interviewees at the branch level expressed a desire for training and guidance related to risk management concepts and their practical application, types of risks to consider, and how to link their specific risk environments and associated decisions to the departmental framework and the CRP.

The absence of formal, standardized, and systemic processes and associated methodologies and tools for effective risk management practices:

- hinder objective identification and assessment of risks;
- inhibit the ability to update risk levels and demonstrate the effectiveness of risk responses and impacts;
- negatively affect the quality and comprehensiveness of risks considered at the branch levels, limiting awareness of emerging risks and the ability to effectively update and integrate risk information at the branch and corporate levels; and
- increase inefficiency and duplication of effort from individual branches that are developing their own risk management frameworks and processes.

The absence of training initiatives, combined with limited or outdated online guidance may also hinder the ability of risk owners and staff to manage risks in alignment with policy expectations.

Conclusion

At the corporate level, HC has developed and implemented tools and methodologies to identify and assess strategic-level risks in the CRP. At branch levels, risk management is considered through operational planning processes, but the Department has not formalized or standardized risk management processes and outputs for branches, such as:

- minimum standards for identifying risks and assigning risk levels (i.e. tools, templates, methodologies); and
- defining and communicating risk tolerances and thresholds, and linking them to risk levels and planned responses.

Development and implementation of targeted risk management training and awareness would support more common and standardized approaches to risks management at the branch level and enhance risk management within the Department.

Recommendation

Recommendation #2:

The CFO, in consultation with branch heads, should develop formal risk management procedures and tools that promote standardized branch-level risk management practices and outputs. To ensure that expectations are understood and activities are implemented consistently, the CFOB should collaborate with branch heads to:

- develop and communicate branch-level risk identification and assessment processes that identify key stakeholders, associated responsibilities, and timelines;
- develop and communicate standard risk categories to be considered in the identification process;
- require branch risk registers to include consideration and assessment of risks to operations, in addition to those in the CRP;
- ensure that branch risk registers are clearly linked to and inform the annual CRP review and update process;
- provide guidance on establishing risk tolerance levels and thresholds, and linking them to risk response and monitoring activities; and
- develop and implement training and awareness informed by results of the periodic assessments of departmental risk management practices.

Criterion 3 – Monitoring

Context

The ongoing monitoring of risks is essential to ensuring that risk information remains relevant. Regular reviews of risk information and risk mitigation measures ensures that changing environmental factors are considered. It also helps ensure that risk responses designed to address issues affecting the organization are effectively implemented and are achieving their desired outcomes.

Monitoring activities also help identify new areas and activities that require attention, and support continual improvement of risk management throughout the organization.

What We Expected To Find

We expected to find systematic processes in place to monitor and report on risks and risk management activities and that these processes integrate and use risk information for decision making.

Key Findings

At the corporate level, risks are monitored on an ongoing basis through periodic updates and presentations to senior executive committees on key initiatives and major projects. Branch activities and underlying risks are linked to core responsibilities and priorities identified in the Departmental Plan (DP) and the Departmental Results Report (DRR). At the branch level, risk responses and underlying risks are monitored through informal bilateral meetings and discussions between managers, directors, and DGs. They are also monitored through mid-year and year-end reviews of operational plans that include, to various degrees, overviews and dashboard presentations to Branch Executive Committees. These discussions also serve to integrate risk information vertically within the Department.

However, as risk management processes across branches are not formalized, there was no systemic approach for monitoring risk management at the branch level. Specifically, there was a lack of documented branch-level risks and risk ratings, as well as a lack of tangible indicators to demonstrate whether risk responses are achieving their expected results. This lack of formal mechanisms may inhibit management's ability to ensure that risk management practices and mitigation measures are being carried out effectively, as well as to:

- effectively allocate efforts and resources;
- consider changing environmental factors on existing risk responses;
- assess the evolution of risks over time and gain insights into emerging risks; and
- ensure that oversight is exercised at the appropriate management level and often enough to support adequate and timely adjustments.

Conclusion

Although the Department has mechanisms in place for monitoring the management of corporate-level risks, there is no formal or systemic approach across branches for doing so. In the absence of regular reviews of risk information, it is difficult to determine whether risk management practices and mitigation measures at all levels of the organization are achieving their desired results. Performance metrics that identify the number of risks, their frequency, and the percentage of risks mitigated, would allow the Department to see the effectiveness of risk management strategies and how they affect the organization, and help ensure that risk monitoring and oversight activities are aligned with risk levels and tolerances.

Recommendations

Recommendation #3

The CFO, in consultation with branch heads, should establish risk management monitoring and assessment processes at the departmental and branch levels to evaluate and demonstrate the effectiveness of risk management activities across the Department and to ensure that risks and their associated responses are periodically reviewed and updated. Elements that would support the development of such processes include identifying and reviewing the following:

- number of risks, whether they materialized, and if they were mitigated;
- changes to the nature and level of risks, and associated responses due to evolving circumstances;
- progress on implementing risk responses; and
- costs of risk mitigation measures.

Appendix A - Scorecard

Audit of Integrated Risk Management – Health Canada			
Criterion	**Risk Rating[2]**	**Risks remaining or forgone opportunities without implementing Recommendation**	**Rec #**
Governance There is an effective governance framework to support IRM throughout the Department.	**3**	Minimum standard requirements for the implementation of processes, use of tools, and for risk management outputs would: • Support the Policy's objective of enabling common approaches and greater consistency, and would enhance oversight and assessment of its application; • Assist individual branches in developing their own risk management policies and frameworks that are aligned with departmental standards; and • Enhance the ability to effectively consider and update risks from all branches and to consolidate and integrate risk information at the corporate level. Defining minimum expectations for risk management across the Department and clarifying the functional role of monitoring risk management practices department-wide would further enhance the responsibilities of branch-level managers and staff, as well as their understanding of these. The lack of more formal and systemic integration of risk management in senior management meetings may inhibit their oversight role and reduce their ability to make informed decisions.	1
Processes Risk management is supported at all levels by established processes, guidance, and tools.	**3**	The absence of more formal, standardized, and systemic processes, methodologies, and tools for the identification of risks, assessment of risk levels, and determination of risk responses, coupled with the absence of minimum requirements for risk management outputs at the branch level, may result in: • A less reliable risk assessment that is repeatable and supportable; • An inability to update risk levels and demonstrate the effectiveness of risk responses and impact on risk; • Adverse impacts on the quality and comprehensiveness of risks considered at the branch levels, limiting awareness of emerging risks and the ability to effectively update and integrate risk information at the branch and corporate levels; and • Inefficiency and duplication of effort as a result of individual branches that are developing their own risk management frameworks and processes. The absence of training, combined with limited or outdated online guidance may hinder the ability of risk owners and staff to manage risks in alignment with policy expectations.	2
Monitoring Systematic processes are in place to monitor and report on risks and risk management activities and to effectively integrate and use risk information for decision making.	**3**	The absence of regular risk monitoring and assessment of risk management practices may inhibit management's ability to: • Objectively determine and demonstrate the effectiveness of risk management responses and initiatives, potentially leading to ineffective responses and misalignment of efforts and resources; • Assess the evolution of risks over time and become aware of emerging risks; and • Ensure that oversight is exercised at the appropriate management level and often enough to better support adequate and timely adjustments.	*3*

1	2	3	4	5
Minimal Risk	Minor Risk	Moderate Risk	Significant Risk	Major Risk

[2] Residual risk without implementing the recommendation.