Audit of Enterprise Risk Management – Public Health Agency of Canada

Final Report

April 2023

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

TO PROMOTE AND PROTECT THE HEALTH OF CANADIANS THROUGH LEADERSHIP, PARTNERSHIP, INNOVATION AND ACTION IN PUBLIC HEALTH.
—Public Health Agency of Canada

Également disponible en français sous le titre :
Audit de la gestion du risque d'entreprise – Agence de la santé publique du Canada

To obtain additional information, please contact:

Public Health Agency of Canada
Address Locator 0900C2
Ottawa, ON K1A 0K9
Tel.: 613-957-2991
Toll free: 1-866-225-0709
Fax: 613-941-5366
TTY: 1-800-465-7735
E-mail: publications-publications@hc-sc.gc.ca

Publication date: April 2023

Cat.: HP5-166/2023E-PDF
ISBN: 978-0-660-67925-9
Pub.: 230417

Executive Summary

Introduction

Effective integration of risk management into an organization's governance, structures, and programs supports decision making and key management functions at all levels of an organization, including policy development, planning and priority setting, resource allocation, and performance assessment.

The Public Health Agency of Canada (PHAC) manages two types of risk: **enterprise risks,** which are the risks that concern the Agency's internal services and administrative objectives, such as HR, funding, and IT capacity; and **public health risks**, which are the risks that concern the health of Canadians. PHAC is in the process of renewing its approach to risk management. Under this new approach, management of public health risks will be led by the Centre of Integrated Risk Assessment (CIRA) within the Corporate Data and Surveillance Branch (CDSB), while enterprise risk management (ERM) will be led by the Enterprise Risk and Planning (ERP) unit within the Chief Financial Officer and Corporate Management Branch (CFOCMB).

Guiding principles for ERM are outlined in various frameworks, including the international risk management standards found in the International Organization for Standardization (ISO 31000) Risk Management Principles and Guidelines, and the Committee of Sponsoring Organizations (COSO)'s Enterprise Risk Management Framework. The Treasury Board of Canada Secretariat's (TBS) Framework for the Management of Risk (2010) also provides broad risk management principles and guidance 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 Agency's risk management framework and practices reflect risk management principles and expectations of the above-mentioned frameworks.

Engagement Objective

The objective of the audit is to determine whether the Agency's enterprise risk management (ERM) framework and practices appropriately support the identification, assessment, and integration of risk information for planning, oversight, and decision-making purposes, and to identify opportunities for improvement as part of the risk management renewal initiative currently in progress.

Engagement Scope

The audit scope focused on fundamental ERM processes and activities at the corporate and branch levels, from April 1, 2019, to March 31, 2022. Specifically, the audit examined policies and governance frameworks, roles and responsibilities, processes, tools, and procedures to identify, assess, and respond to risks, as well as processes for monitoring and reporting risk information and integrating it in the Agency's planning and reporting cycles. The scope did not include an assessment of the Agency's approach to managing public health risks, of the appropriateness of the risks identified, nor of the actual risk levels or ratings and the responses determined by management.

What We Found

During the years prior to the onset of COVID-19, PHAC had a robust process for formally identifying and assessing its strategic risks through its Corporate Risk Profile (CRP) process. Our review suggests that the CRP and associated risk management processes were well supported through activities like benchmarking exercises, risk management workshops, training initiatives, and risk capability model assessments. This was further enabled with tools like risk participant and desk guides, risk management tip sheets and questionnaires, and a voting software to facilitate risk assessment and compilation. There was also a dedicated Risk Management Oversight Committee for risk management practices across the Agency.

Since the onset of COVID-19, and until the realignment of ERM responsibilities in 2021, there was limited centralized leadership to support and coordinate ERM, as well as a lack of formal processes, tools, and training to support common ERM practices. PHAC did not update and approve its CRP during this time. This can be attributed to the following:

- ➢ shifting priorities and the impact of COVID-19 on all aspects of the Agency's operations and resources;
- ➢ organizational and operational complexities brought on by the Agency's significant expansion and reorganization; and
- ➢ the transition of responsibilities for leading ERM from the Strategic Policy Branch (SPB) to the Chief Financial Officer and Corporate Management Branch (CFOCMB) during this time.

Since the responsibility for leading ERM was transferred to CFOCMB in late 2021, the Agency has re-focused its efforts on risk management practices and bolstered its capacity by establishing the Enterprise Risk and Planning (ERP) unit. This unit is leading an ERM approach to enhance the risk management framework and practices across the Agency. As designed, the approach includes appropriate risk management guidance, well-defined governance structures, and more formalized processes for the identification, assessment, response, and monitoring of risks. In moving forward with the new approach and implementation of the risk management framework for ERM, the Agency should do the following:

- standardize risk management processes and tools, and establish baseline expectations for risk management outputs and deliverables for branches and corporate functional units through the Integrated Risk Management Guidelines;
- ensure that senior management oversight is supported through regular reviews, assessments, and reporting on the status of ERM practices via the annual Corporate Risk Profile review;
- establish and implement more robust risk monitoring and reporting processes and practices that:
  - ○ are aligned with the severity of risks and established risk tolerances;
  - ○ adequately identify risk monitoring information requirements; and
- support the ongoing identification, assessment, and discussion of the impact of risk responses on underlying risks through the establishment of a Corporate Risk Register.

Criterion 1 - Governance

Context

Integrating risk management into governance processes supports management in delivering its mandate by facilitating faster and better-informed decisions, informing the best allocation of resources, and supporting compliance with policies and legislation. It also helps the Agency to recognize, understand, accommodate, and capitalize on new challenges and opportunities, and also 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 scope of this audit. The absence of MAF assessments of integrated risk management, combined with the volatile and resource-intensive COVID-19 operating environment may have adversely affected the focus and engagement on risk management in recent years.

What We Expected To Find

We expected to find that appropriate governance frameworks support ERM throughout the Agency, including established policies and standards, clearly defined roles and responsibilities, and appropriate bodies to provide direction and oversight.

Key Findings

Policy and Directives

The PHAC Integrated Risk Management Policy (the Policy) and Integrated Risk Management Guideline (the Guideline) have been developed to update or replace the pre-existing *Integrated Risk Management Standard* (2009) and former *IRM Policy* (2013). The guidance provided in the newly developed documents is consistent with, and reflects the key elements of the *TBS Framework for the Management of Risk.* The Policy outlines general expectations related to risk management and clearly sets out roles and responsibilities for both ERM and health-related risks for the President and Branch Heads, the CPHO, the CIRA, key organizational units and governance committees, as well as executives, managers, and employees.

To further enhance the Policy and Guideline, the Agency should consider the following:

- identifying common baseline expectations for all branches and functional units for risk management processes and deliverables and their supporting documentation;
- assigning responsibility for reviewing, assessing, and reporting on ERM practices and their alignment with policy expectations; and
- more robust guidance on key elements and considerations in developing effective risk monitoring and reporting plans and practices.

Incorporating the considerations above would support a common understanding of risk management expectations, establish consistent practices, and facilitate oversight and assessment of Policy implementation. Furthermore, it would enhance the Agency's ability to consolidate and integrate risk information across branches and functional units.

Roles and Responsibilities

The newly developed Policy clearly defines risk management roles and responsibilities at all levels of management and for key governance bodies. As stated above, an opportunity exists to identify the responsibility more clearly for ongoing monitoring, assessment and reporting of risk management practices and their alignment with policy requirements. This would support the Agency in the timely assessment of the risk management framework and in taking corrective actions when required.

Effective communication of these roles and responsibilities is expected to take place via the newly constituted Enterprise Risk Management Network, and planned training and outreach initiatives led by the ERP unit.

Governance Bodies

Overall, the Agency's governance committees are effectively engaged in reviewing and discussing risks at all levels and on an ongoing basis. Although risk management-specific discussions are not a standing item on agendas, they are typically integrated within other activities, including presentations of plans and priorities, status reports on initiatives, and various ad hoc presentations on key projects and initiatives.

The approach for risk management oversight by senior committees could be further standardized at the branch and corporate levels. This would include identifying key risk-related information and reporting tools to be presented and discussed with some regularity at governance committees. These requirements should be clearly defined in the risk monitoring and reporting plans and aligned with guidance provided by the ERP unit. It is expected that further development and full implementation of the current ERM approach will address this opportunity for improvement.

Conclusion

As designed, the updated ERM approach should adequately address key elements of risk management governance. To further support the implementation of the new approach and sound risk management practices and oversight, the Agency should consider clarifying baseline risk management expectations and risk monitoring processes for branches and functional units.

Recommendation 1

The CFO should ensure that the Agency's Integrated Risk Management Policy and Guideline, which are currently under development, do the following:

- Clearly establish baseline risk management expectations and deliverables for branches and functional units; and
- Clarify the roles and responsibilities for ongoing monitoring and reporting on Agency risk management practices and adherence to Policy expectations.

Context

Integrated Risk Management, including management of enterprise risks, 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 to aggregate risk information at the corporate level to better address challenges facing the organization.

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

This would in turn facilitate the monitoring and implementation of risk management processes across the Agency.

What We Expected To Find

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

Criterion 2 – Risk Management Processes

Key Findings

The CRP is the key risk management process used to identify and document strategic corporate enterprise risks that could affect the achievement of the Agency's mandate. It identifies risks over three-year cycles, with a requirement for annual reviews and updates. Although there is evidence that the Agency previously had a robust review and renewal process in place, the most recent updates to the CRP took place prior to the onset of the COVID-19 pandemic and were not approved by the Executive Committee. This could be attributed to the volatile and resource-intensive pandemic environment, and a limited central risk management function during that time. Notwithstanding the absence of an updated and approved CRP during the period under review, there was evidence that enterprise risks were being considered and addressed through functional area planning activities, including risks related to HR, business continuity, IM/IT, and real property and security. However, these efforts were made across various teams with minimal coordination and integration across branches or the Agency as a whole. While risks were implicitly and explicitly addressed through planning activities, there were generally no formal processes that documented the identification and assessment of enterprise-wide risks. We have noted that, at the time of this audit, the 2022 to 2025 CRP process is currently in progress, with an expectation that it will be tabled for approval in late winter of 2023.

At the branch level, risk management practices are generally included in operational planning and reporting processes. Interviewees indicated that risk management is also considered informally as part of regular and ongoing bilateral or multilateral meetings between DGs, directors, and managers. Although risks are considered in operational planning and reporting processes, there was little evidence of formal and systematic branch-level risk frameworks and processes to identify risks, as well as assign risk levels, risk responses, or monitor risks, including use of templates, risk registers, risk scales, 'heat maps', and risk tolerance matrices. We also found that the previously used operational planning processes that supported risk management varied in format and application among branches, and were not used consistently. This may have impeded the consolidation and consideration of branch-level enterprise risks at the corporate level. However, the most recent planning and reporting cycle (2022-23) includes significant steps to formalize and standardize operational planning processes across the Agency. There was evidence of use of a standardized operational planning template that formally links operational planning priorities and activities to risks at the Agency, branch, and directorate levels.

The Agency does not currently offer formal training on risk management, and website guidance is limited. Interviewees indicated that risk management is intuitive and practiced implicitly, and that risk consideration drives all decisions. However, some interviewees also expressed interest in training and guidance on corporate risk management expectations and in linking their specific risk environments and associated decisions to strategic-level corporate risks. The current ERM approach commits to a communication strategy and learning and development activities that Policy expectations, including ERM training workshops, updates to the PHAC intranet site, and the launch of a Branch Risk Register process. The newly-formed Enterprise Risk Management Network, headed by CFOCMB's ERP unit, in collaboration with representatives from branches and functional areas, is expected to be an effective mechanism in supporting planned enterprise risk management training and awareness initiatives.

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

- adverse impacts on the quality and comprehensiveness of risk information at the corporate and branch levels;
- a continued lack of clear and objective determination of risk to facilitate risk level assignment and measure and identify the effectiveness of risk responses;
- limiting the ability to effectively integrate and align risk management information vertically and horizontally across the Agency; and
- the development of individual risk management frameworks and practices by branches and functional units that may result in inefficiency and duplication of efforts within the Agency.

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

Conclusion

The overall lack of rigorous and standardized risk management processes during the audit period was the result of the Agency's focus on the COVID-19 pandemic, coupled with the impact of organizational restructuring initiatives and shifting ERM responsibilities.

However, the updated ERM approach and associated initiatives led by the ERP unit provide a solid foundation for ERM processes moving forward. The newly implemented operational planning process, though not yet fully established, nor tested, is a strong component of an overall ERM process and should be effective in formally integrating risks into operational plans at all levels. The draft Policy and Guideline, together with additional planned guidance, training, and communication activities by the ERP unit, are expected to provide sufficient formalization and a level of standardization in the overall risk management processes of the Agency.

Recommendation

None – Recommendations 1 and 2 adequately address identified opportunities for improvement to the ERM processes and tools in the Agency.

Criterion 3 – Monitoring

Context

Ongoing risk monitoring is essential to ensuring that risk information remains relevant and that changes to the risk environment are considered. It also helps ensure that risk responses designed to address issues affecting the organization are effectively implemented and achieve their desired outcomes.

Furthermore, monitoring activities help identify new areas and activities that require oversight, 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, the Departmental Plan (DP) and Departmental Results Report (DRR) outline and discuss key priorities and associated results. This includes planned results for internal services functional areas such as HR, IT, and Finance. While the DP and DRR present periodic updates to senior management on key initiatives and major projects, there are no explicit links between the impact of underlying ERM risks on planned priorities.

At the branch level, risk responses and underlying risks are monitored through informal bilateral meetings and discussions between managers, directors, and DGs, and through mid-year and year-end reviews of operational plans. However, as risk management processes across branches are not sufficiently formalized, there is no systematic approach for monitoring the management of risks and assessing the effectiveness of risk responses. Specifically, there is a lack of documented branch-level risks and risk ratings, and a lack of tangible indicators to demonstrate whether risk responses are achieving their expected results.

As previously noted, although not yet fully adopted across all branches, the Agency's operational planning processes have been significantly strengthened during the 2022-23 planning cycle. Once fully implemented, the CFOCMB's ERP unit aims to enhance risk monitoring by implementing a standardized process for discussing risk issues across all levels of the Agency.

A lack of formal and systematic approaches to monitoring ERM risks inhibits management's ability to do the following:

- objectively determine and demonstrate the effectiveness of risk management responses and initiatives;
- assess the evolution of risks over time and gain visibility into emerging risks; and
- ensure that oversight is exercised at the appropriate management level and frequently enough to support timely and appropriate risk responses and necessary adjustments.

Conclusion

The Agency's processes and mechanisms to monitor and report on risks have been informal and inconsistent. The Agency is developing more sound risk monitoring processes as part of its ERM update and the current operational planning processes and tools will support risk integration into the planning processes across the Agency. Areas where opportunities exist to further strengthen the monitoring and reporting processes include:

- Formally documenting the identification and assessment of risks, which is to be addressed through minimum expectations referred to Recommendation 1;
- More formal and systematic approaches to ongoing risk monitoring in order to enhance management's ability to assess the extent to which responses mitigate risks to within established tolerances; and
- Implementing formal oversight of risk management by senior management committees through more structured reporting of risk-specific information on a regular basis, consistent with guidance to be developed, pursuant to recommendation 1.

Recommendation 2

The CFO, in consultation with branch heads and functional area leads, should develop and provide guidance for establishing more robust risk monitoring and reporting processes, including the following:

- ongoing assessment and consideration of the impact of responses on underlying risks;
- aligning monitoring and reporting activities with severity of risks and established tolerance levels; and
- defining risk information requirements in support of monitoring and reporting plans and processes.

Appendix A – Scorecard

Audit of Enterprise Risk Management – Public Health Agency of Canada

Criterion	Risk Rating[1]	Risks remaining or forgone opportunities without implementing the Recommendations	Rec #
Governance There is an effective governance framework to support ERM throughout the Agency.	3	• The lack of updated, relevant, and clear policy requirements and associated guidance increases the possibility that expectations for risk management will not be clearly and commonly understood across the Agency, and that risk management will not be practiced in alignment with Agency policy. Furthermore, it may also hinder the Agency's ability to effectively assess if risk management practices are consistent with Agency expectations. • The lack of formal and systematic and ongoing assessment and oversight of risk management practices that are compliant with policy expectations outlined in senior management governance structures may undermine the perceived importance of risk management in the Agency. It may also adversely affect accountability for risk management, as well as the ability of senior management to effectively identify and respond to risk trends or emerging risks in a timely manner.	1
Processes Risk management is supported at all levels by established processes, guidance, and tools.	3	The absence of more formal and structured processes and associated outputs for risk management increases the risk of the following: • adverse impacts on the quality and comprehensiveness of risk information at the corporate and branch levels; • hindering a more objective risk determination process that is repeatable and supportable, and the ability to update risk levels and facilitate the demonstration of the effectiveness of responses and their impact on risks; • limiting the ability to effectively integrate and align RM information vertically and horizontally across the Agency; and • development of individual RM frameworks and practices by branches and functional units that may result in inefficiency and duplication of efforts across the Agency. The absence of training initiatives, combined with limited or outdated website guidance, may hinder the ability of risk owners to manage risks effectively and in alignment with departmental expectations. Lack of training may also contribute to inconsistency in practices and outputs that could hinder effective integration of risk information.	1
Monitoring Systematic processes are in place to monitor and report on risks and risk management activities and for effectively integrating and using risk information for decision-making	3	The absence of more formal and systemic monitoring and reporting plans and processes may inhibit management's ability to do the following: • Objectively determine and demonstrate the effectiveness of risk management responses and initiatives; • Assess the evolution of risks over time and gain perspective on emerging risks; and • Ensure that oversight is exercised at the appropriate management level and frequently enough to better support timely and appropriate risk responses and necessary adjustments.	2

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

[1] Residual risk without implementing the recommendation.

Appendix B – About the Audit

1. Audit Objective

The objective of the audit was to determine whether the Agency's enterprise risk management (ERM) framework and practices appropriately support the identification, assessment, and integration of risk information for planning, oversight, and decision-making purposes, and to identify opportunities for improvement as part of the risk management renewal initiative currently in progress.

2. Audit Scope

The audit scope focused on fundamental ERM processes and activities at the corporate and branch levels, from April 1, 2019, to March 31, 2022. Specifically, the audit examined policies and governance frameworks, roles and responsibilities, processes, tools, and procedures to identify, assess, and respond to risk, as well as processes for monitoring and reporting risk information and integrating it into the Agency's planning and reporting cycles. The scope did not include an assessment of the Agency's approach to managing public health risks, the appropriateness of the risks identified, or of the actual risk levels or ratings, nor the responses determined by management.

The audit also reviewed select documentation from before 2019 on ERM activities and processes in place. Its purpose was to identify strong practices for CFOCMB's consideration in support of an effective and efficient renewal of risk management processes.

3. Audit Approach

The audit was conducted in accordance with the Government of Canada's *Policy on Internal Audit*, which requires examining sufficient and relevant evidence, and obtaining sufficient information and explanations to provide a reasonable level of assurance in support of the audit conclusion.

The audit approach included, but was not limited to the following:

- Interviews with management, committee members, and key stakeholders within corporate and branch organizational units;
- Review of processes and methodologies, and examination of outputs and other relevant supporting documentation; and
- Testing of controls as required.

To identify opportunities for improvement as part of the risk management renewal initiative, the audit also adopted an agile audit approach. This approach enabled the audit team to review and comment on draft documents as they were being developed and provide feedback in a timely manner.

4. 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.

5. Audit Criteria

The audit criteria were derived from the TBS Framework for the Management of Risk, the TBS Guide to Integrated Risk Management, the International Organization for Standardization Risk Management Principles, and the Committee of Sponsoring Organizations' Enterprise Risk Management Framework. The following audit criteria were used to conduct the audit ted risk management:

Audit of Enterprise Risk Management	
Audit Criteria	
1	There is an appropriate governance framework, which is aligned with TB guidance and principles, to support ERM throughout the Agency.
2	Enterprise risk management is supported at the Agency, branch, and directorate levels by established processes, guidance, and tools.
3	Systematic processes are in place to monitor and report on enterprise risks and risk management activities, and to effectively integrate and use risk information for decision-making and planning purposes.