Public Service Commission of Canada
Commission de la fonction publique du Canada

Audit of Risk Management Practices

Canada

Table of Contents

1. Executive summary

This audit assessed whether the Public Service Commission of Canada (PSC) has risk management practices that contribute to the sound management of its activities and that support senior managers in decision-making.

The internal audit team shared preliminary findings with the Executive Management Committee, and some modifications were made to PSC risk management practices during the fall of 2022. These changes were not within the scope of this audit.

Some good risk management practices are in place at the PSC, such as:

- The PSC has a process to identify and communicate key corporate risks.
- Roles and responsibilities are well defined within the governance structure of the PSC for the corporate risk identification process.
- The PSC has a process in place to identify and report on deliverables of mitigation strategies.
- The PSC has tools to support the identification of corporate risks.

However, this audit concludes that risk management practices at the PSC are insufficient to support sound management and decision-making and that improvements are required to support good risk management practices.

These practices do not support risk management and sound decision-making:

- The risk identification process fails to identify all important corporate risks and to support in-year updates.

    - Risk rating [1] : High
    - Recommendation 1: The Vice-President of the Corporate Affairs Sector, in collaboration with the Executive Management Committee, should implement an enterprise risk management framework that includes a clear

[1] The risk rating describes the level of impact and likelihood (combined) that risk management practices will not support sound public management and informed decision-making if the recommendations are not taken into consideration. A “high” risk rating means that the internal audit team expects prompt implementation of the action plan following the recommendation. Implementation of recommendations should be prioritized based on the risk rating.

process to identify, track and update key corporate risks. They should also ensure that enough time is allocated to identify and discuss risks.

  - Response: The Vice-President of the Corporate Affairs Sector supports the recommendation to adopt an enterprise risk management framework. Risk management is a critical component of the integrated planning approach, through regular engagement with sectors, directorates and the PSC.
  - Planned actions: An enterprise risk management framework will be developed in line with the Treasury Board of Canada Secretariat's risk management framework. The framework will include a process to ensure quarterly monitoring as well as regular discussions at governance committees.

- Some identified corporate risks are issues.
  - Risk rating: High
  - Recommendation 2: The Results and Delivery Division should include a list of key issues and action plans in the planning process, separate from the risks and mitigation strategies list.
  - Response: The Vice-President of the Corporate Affairs Sector supports the recommendation.
  - Planned actions:

- As part of the integrated planning approach, regular meetings with sectors and directorates will allow for identification of key issues and action plans.
- As part of the integrated planning approach, sectors and the Executive Management Committee will be provided with key issues, risks and risk responses and mitigation strategies for review and discussion.
- Corporate risk ownership for the day-to-day management is not clearly delegated.
  - Risk rating: High
  - Recommendation 3: As part of the enterprise risk management framework, the Results and Delivery Division, in collaboration with the Executive Management Committee, should build a process to designate risk ownership for each specific risk and ensure accountability, including monitoring and ensuring a response aligned with the appetite of senior management.

  - Response: The Vice-President of the Corporate Affairs Sector supports the recommendation.
  - Planned actions: Roles and responsibilities of risk owners will be clearly identified as part of the risk framework.
- There are no controls in place to measure the effectiveness of mitigation strategies.
  - Risk rating: High
  - Recommendation 3 and planned actions support this finding.
- Risk appetite and risk tolerance are not clearly communicated throughout the PSC.
  - Risk rating: High
  - Recommendation 4: The Results and Delivery Division, in collaboration with the Executive Management Committee, should ensure that the enterprise risk management framework includes a process to clearly identify and communicate the Executive Management Committee's risk tolerance and appetite to PSC employees.
  - Response: The Vice-President of the Corporate Affairs Sector agrees that an enterprise risk management framework should include a communication strategy to inform PSC employees.
  - Planned actions:
- Develop a communications plan in collaboration with the communications team to ensure the most effective way to inform PSC employees about senior management's risk tolerance.
- The Results and Delivery Division, in collaboration with Communications and Parliamentary Affairs Directorate, will develop an Intracom page containing planning, reporting, risk and performance measurement information.
- There is a lack of support for risk management at the operational level.
  - Risk rating: Medium
  - Recommendation 5: The Vice-President of the Corporate Affairs Sector should identify a group that will be responsible for promoting available tools and training to support a risk management culture.

- Response: The Vice-President of the Corporate Affairs Sector agrees with the recommendation.
- Planned actions:

- The Results and Delivery Division will be responsible for promoting tools and training to support a risk management culture.
- The Results and Delivery Division will collaborate with the Human Resources, Workplace and Security Directorate to include relevant risk training in the PSC's learning catalogue.

2. Introduction

Background

What is risk management

Risk is defined as "the effect of uncertainty on objectives." It is generally expressed, and its importance is measured, by considering the probability and the possible repercussions. Risks are different from existing problems and issues for which there are certainties. Although risk is often perceived as negative, it can have a positive impact and present opportunities to be leveraged.

Risk management, as defined by the Treasury Board of Canada Secretariat, is a systematic, continuous and proactive approach to understanding, managing and communicating risks from an organization-wide and business/project perspective. It is part of sound public management because it promotes informed decision-making, based on an understanding of risk, planned mitigation strategies and leveraging of opportunities.

Overall, good risk management supports the achievement of organizational objectives. The Treasury Board of Canada Secretariat views effective risk management as an essential component to improving the way public servants deliver services to Canadians, capitalize on opportunities and focus on results.

Because federal departments and agencies have different objectives and operational contexts, it is up to each of them to implement risk management practices adapted to their needs that include risk identification, assessment, processing, monitoring and communication.

Risk management at the Public Service Commission of Canada

The COVID-19 pandemic has tested the ability of departments and agencies to adapt to a rapid changing environment and new emerging risks. The Public Service Commission of Canada (PSC) has not been spared from the uncertainty. It has been forced to find new ways to deliver its programs and services despite COVID-19 impacts on the workplace. After more than 3 years, remaining uncertainty has been exacerbated by strong competition for labour and the transition to a hybrid work model.

Under these conditions, the PSC needs to have good risk management practices that contribute to the sound management of its activities and that support senior management in decision-making. Failure to manage risks effectively can slow down initiatives, jeopardize projects, increase the cost of programs, create reputational damage and ultimately undermine the ability of the PSC to deliver on its mandate.

Audit objective and scope

This audit aimed to assess whether the PSC has risk management practices that contribute to the sound management of its activities and support senior managers in decision-making. The internal audit team considered the size of the PSC, its operating context and mandate. More specifically, the audit looked at:

- the effectiveness of the integrated risk identification process, including the analysis and communication of risks to support informed decision-making
- the effectiveness of the governance and practices that support activities related to risk management, including roles, responsibilities and accountability
- the effectiveness of controls for risk response, their implementation, accountability for results and alignment of practices with senior management risk tolerance
- the availability of expertise and tools to support good risk management practices, including at the operational level

These objectives are aligned with the expectation of the Institute of Internal Auditors, requiring that internal audit teams regularly assess the effectiveness of risk management practices and processes within their organization, and contribute to their improvement.

The audit focused on risk management activities at the PSC between April 2018 and September 2022. The lengthy period was selected to allow for an understanding of patterns and practices that are not always documented in small organizations like the PSC. The internal audit team shared preliminary findings with the Executive

Management Committee, and some modifications were made to PSC risk management practices during the fall of 2022. These changes were not considered in this audit.

Methodology

We used the following methods for this audit:

- conducted 20 interviews with stakeholders responsible for risk management at the PSC and senior management, including directors general and vice-presidents
- reviewed relevant documents and files
- assessed a sample of projects and activities to identify and understand trends at the operational level:
    - GC Jobs Transformation
    - the Second Language Evaluation – Unsupervised Internet Testing Project
    - the Priority Entitlement Program

Statement of conformance

The audit is in conformance with the Internal Audit Standards for the Government of Canada as supported by the results of the quality assurance and improvement program.

3. Findings and recommendations

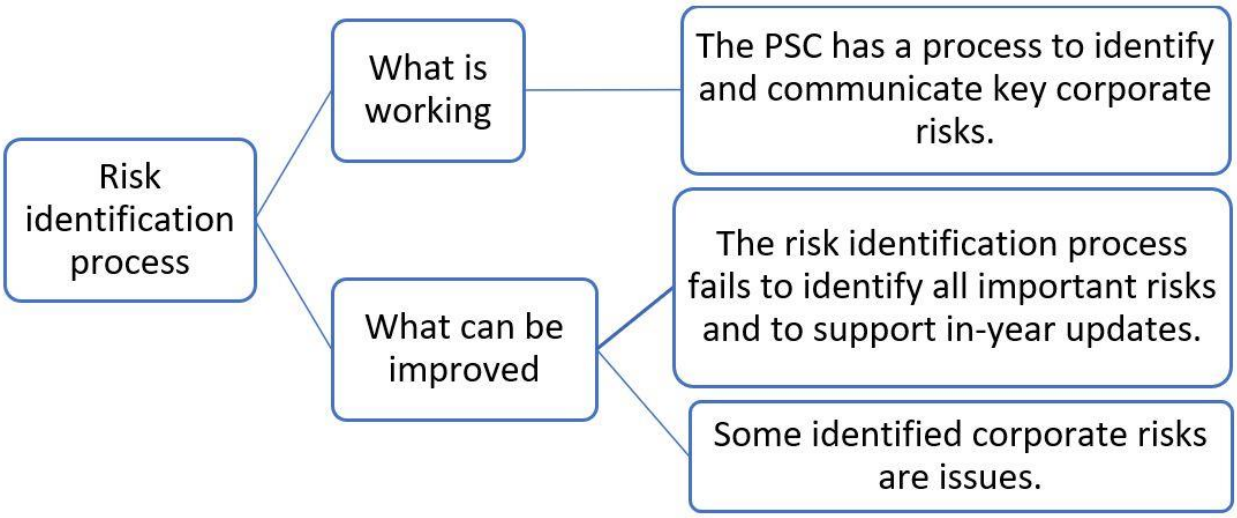
3.1 Risk identification process

The PSC risk identification process does not support effective risk management and decision-making.

What we looked at and why it matters

The internal audit team assessed whether the PSC has a process to identify risks that can impact its mandate and objectives. The team also assessed whether identified risks were communicated to senior management in a timely manner to support decision-making. Risk identification enables the PSC to develop responses that minimize harmful situations before they arise, or to take advantage of opportunities. It also supports strategic planning of activities.

Findings



Text version

This is a chart summarizing the findings of the Risk Identification Process section of the report.

The first box of the chart is titled "Risk identification process." Linked to this box are 2 boxes titled "What is working" and "What can be improved." Linked to the "What is working" box, another box presents this finding: "The PSC has a process to identify and communicate key corporate risks." Linked to the "What can be improved" box, 2 other boxes present these findings: "The risk identification process fails to identify all important risks and to support in-year updates" and "Some identified corporate risks are issues."

What is working

The PSC has a process to identify and communicate key corporate risks.[2]

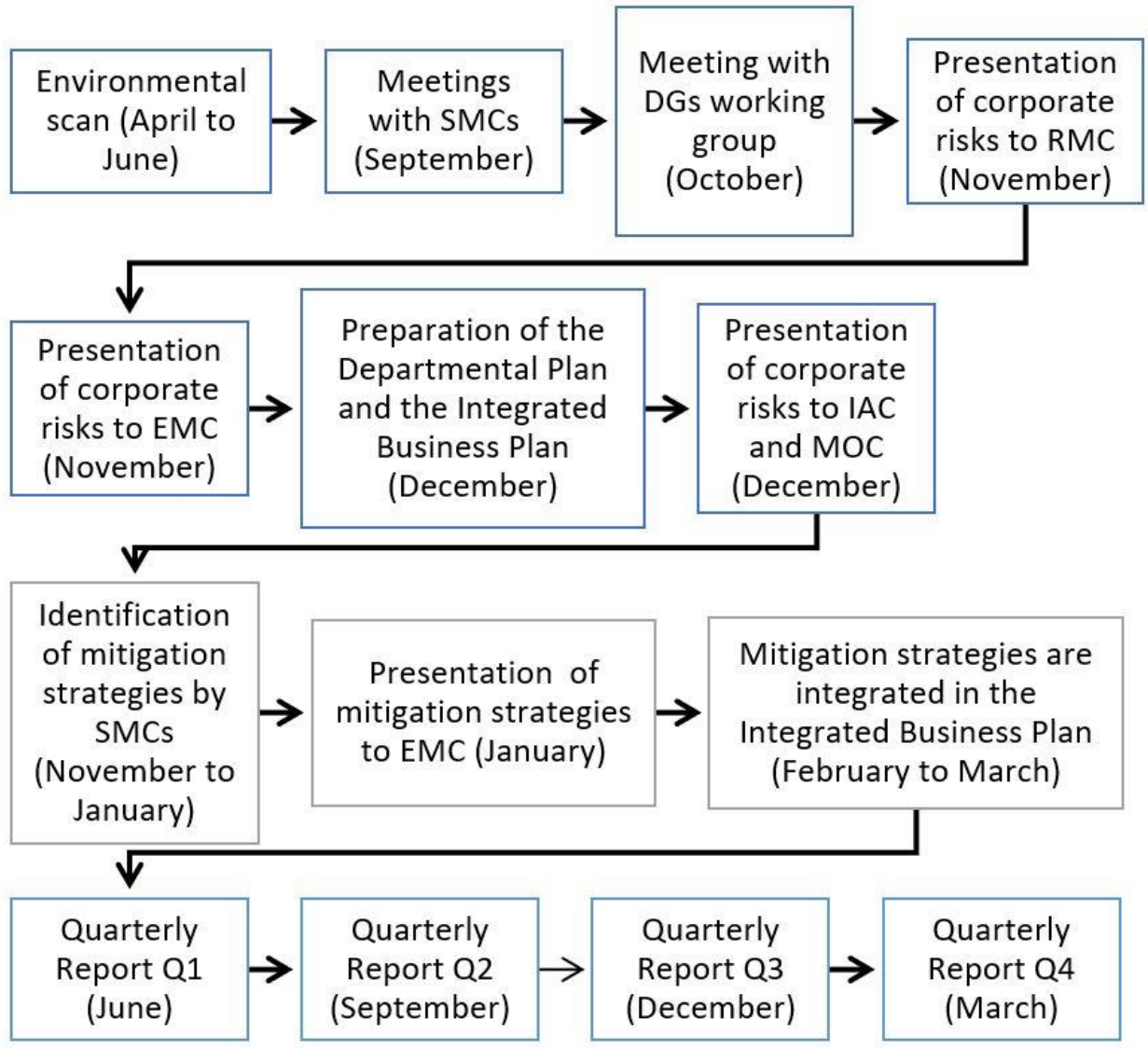
The internal audit team found that the PSC has a process for identifying and communicating its key corporate risks. Even if this process is not part of an official framework, it has been similar throughout most of the period covered by the audit (fall 2018 to fall 2022). Annually, the Results and Delivery Division meets with sector

[2] The internal audit team noticed that in the period following the scope of the audit, changes were made to the process. The 2023–24 corporate risks were identified and validated only by the Executive Management Committee at a retreat in October 2022. Vice-presidents were required to discuss about risk with their sector management committees before Executive Management Committee meetings and the retreat.

management committees to discuss risks related to achieving the annual priorities. Afterwards, an informal committee of directors general meets to discuss and identify the most important ones. These risks are then discussed at the Resource Management Committee. Finally, these risks are presented to the Executive Management Committee for approval and are integrated into the Departmental Plan and the Integrated Business Plan. The risks are also shared with sectors to help them plan for the next fiscal year and for information to the Internal Audit Committee and at the Meetings of the Commission (see the following table for the full cycle).

Every quarter, sectors can propose changes to the list of risks when information is collected for the quarterly update by the Results and Delivery Division in the Corporate Affairs Sector. Changes could be discussed at the Resource Management Committee and proposed to the Executive Management Committee.

Corporate risk management cycle



Text version

This is a flowchart summarizing the steps of the corporate risk management cycle at the PSC. There are 14 boxes that follow each other in this order:

1. Environmental Scan (April - June)
2. Meetings with sector management committees (September)
3. Meeting with directors general working group (October)
4. Presentation of corporate risks to Resource Management Committee (November)
5. Presentation of corporate risks to Executive Management Committee (November)
6. Preparation of the Departmental Plan and the Integrated Business Plan (December)

7. Presentation of corporate risks to Internal Audit Committee and Meeting of the Commission (December)
8. Identification of mitigation strategies by Sector Management Committees (November - January)
9. Presentation of mitigation strategies to Executive Management Committee (January)
10. Mitigation strategies are integrated in the Integrated Business Plan (February - March)
11. Quarterly Report Q1 (June)
12. Quarterly Report Q2 (September)
13. Quarterly Report Q3 (December)
14. Quarterly Report Q4 (March)

Note: This table uses the following abbreviations: Sector Management Committee (SMC); Director General (DG); Resource Management Committee (RMC); Executive Management Committee (EMC); Internal Audit Committee (IAC); Meeting of the Commission (MOC).

What can be improved

The risk identification process fails to identify all important corporate risks and support in-year updates.

The internal audit team found that the current risk identification process is not effective in identifying emerging risks and ensuring proper oversight of corporate risks.

- Only 3 to 4 corporate risks are identified every year
    - during interviews with senior managers, key risks that were not on the official corporate list were raised with the internal audit team and described as having the potential to impact PSC's objectives (refer to causes for an explanation)
- Even if sectors can propose in-year updates to the risk list, including instances of new risks emerging, they have not done so during the period covered by the audit

- Most directors general and vice-presidents reported a preference to report risks to colleagues using other mechanisms than the formal process, such as informal or topic-specific discussions (for example, on GC Jobs Transformation or Second Language Evaluation-Unsupervised Internet Testing) at Sector Management Committees, Executive Management Committee or through informal discussions with their immediate supervisor (vice-presidents or President)

As a result, as some senior managers also expressed, the risk identification process is insufficient to ensure that every important risk is tracked.

Causes

A key cause of this situation is that the Departmental Plan limits the number of high-level significant corporate risks to 3 or 4. Risks are formulated to be communicated to the public. These risks are then copied in the Integrated Business Plan and tracked quarterly (via quarterly monitoring), without modification or addition of other existing or emerging corporate risks. As a result, the list is incomplete.

Another cause is the lack of time allocated to formally discuss risks at various governance committees. Excluding the annual discussion about risks at the Executive Management Committee's fall retreat, risk-related discussions occur with other important organizational topics such as annual deliverables, PSC results, financial situation and status of resources. This results in risk-related discussions competing for enough time during committee meetings.

The internal audit team also found that the risk management approach at the PSC, including the risk identification process, has never been adopted as an organization-wide solution for risk management. For this reason, expectations about when and how to report risks are not always clear for stakeholders.

Consequences

- Key risks may not be identified in a timely manner, impacting the response and the achievement of PSC objectives
- Key risks are not communicated consistently across the PSC

Adopting a structured and consistent enterprise risk management framework, including a formal risk identification process, would:

- bring consistency
- improve the value proposition of risk management
- help manage uncertainties
- make the most of opportunities

"Enterprise Risk Management is a structured, consistent process that benefits the entire organization by identifying, assessing, deciding on responses to, and reporting on opportunities and threats that affect an organization's objectives. […] [It] is used throughout organizations for identifying strategic risks and for developing business practices to avoid surprises from those same that can lead to project failure, scandals, or significant damage to the organization." (Institute of Internal Auditors)

Adopting an enterprise risk management framework is recognized as a best practice by sources of authority, including the Chartered Professional Accountants of Canada and the Institute of Internal Auditors. This also applies to small organizations like the PSC.

Recommendation 1

The Vice-President of the Corporate Affairs Sector, in collaboration with the Executive Management Committee, should implement an enterprise risk management framework that includes a clear process to identify, track and update key corporate risks. They should also ensure that enough time is allocated to identify and discuss risks.

Some identified corporate risks are issues.

Most senior managers interviewed expressed concerns that corporate risks have materialized into issues. Resource Management Committee meeting minutes show that this problem was discussed as early as 2019 but has not been resolved.

"Risk is about the effect of uncertainty, and therefore future-oriented, risks are distinct from existing issues, problems, or business conditions, where likelihood of occurrence would not be an issue." (Treasury Board of Canada Secretariat, Guide to Integrated Risk Management)

Causes

During our interviews, some senior managers stated that these issues are too important to simply be removed from the list. There are currently no other tools at the PSC to track these issues and their action plans.

Also, the internal audit team found that risk statements are not always clear and do not follow the best practices recommended by Treasury Board of Canada Secretariat, including identifying the event and impact. PSC identified risks are often broad in nature, it often isn't clear why they are considered to be threats, and the impact is not always assessed. This can create confusion between current events, issues and risks.

"A risk statement would describe the event and the potential impact (positive or negative) of that event on achieving an organization's objectives."

"An event is a situation, occurrence or change in a particular set of circumstances that has the potential to affect the achievement of an organization's objectives. An event may be positive or negative.

An impact is the potential effect of an event. As with an event, an impact may be positive or negative."

"A suggested method for developing a risk statement for a threat involves at least two elements: the event itself and the potential negative impact of such an event if left unmanaged.

Risk statement (threat): If (event) occurs, the consequences could result in (negative impact)." Treasury Board of Canada Secretariat, Guide to Risk Statements)

Consequences

This situation limits the PSC's ability to:

- focus on real risks that have the potential to become issues
- identify proper mitigation strategies for risks
- develop proper action plans for issues

Recommendation 2

The Results and Delivery Division, in collaboration with the Executive Management Committee, should include a list of key issues and action plans in the planning process, separate from the risks and mitigation strategies list.

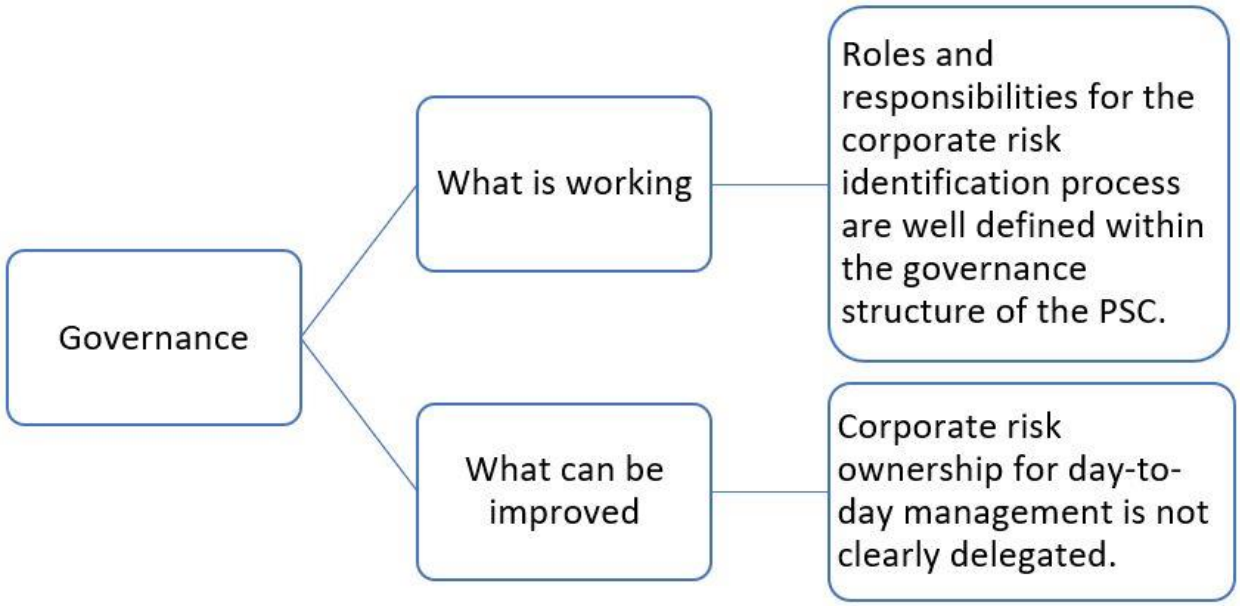
3.2 Governance: roles, responsibilities and accountabilities

Corporate risk ownership is not clearly delegated to an individual or a role for day-to-day management and accountability purposes; this does not support risk management and decision-making.

What we looked at and why it matters

The internal audit team assessed whether the PSC has an effective risk management governance, including a clear designation of roles, responsibilities and accountabilities. This is important to ensure risks are properly assessed, discussed and managed. It also helps ensure that the response is aligned with senior management's appetite for risk. Proper risk governance reduces the risk of the PSC not achieving its objectives.

Findings



Text version

This is a chart summarizing the findings of the Governance: Roles, Responsibilities and Accountabilities section of the report.

The first box of the chart is titled "Governance." Linked to this box are 2 boxes titled "What is working" and "What can be improved." Linked to the "What is working" box, another box presents this finding: "Roles and responsibilities for the corporate risk identification process are well defined within the governance structure of the PSC." Linked to the "What can be improved" box, another box presents this finding: "Corporate risks ownership for day-to-day management is not clearly delegated."

What is working

Roles and responsibilities for the corporate risk identification process are well defined within the governance structure of the PSC.

The responsibilities for risk management at a corporate level are integrated into the PSC's governance, as defined by the terms of reference for the Resource Management Committee and the Executive Management Committee. The Results and Delivery Division facilitates the processes by collecting information on risks and reporting on them regularly, through the Integrated Business Plans, departmental plans, departmental results reports and quarterly updates. The team is responsible for managing key steps of the risk identification and reporting processes, including identifying mitigation strategies, and reporting quarterly on risks and mitigation strategies at the Resource Management Committee and the Executive Management Committee.

What can be improved

Corporate risk ownership for day-to-day management is not clearly delegated.[3]

The Results and Delivery Division is responsible for conducting the key steps of the risk identification and reporting process, as identified in section 3.1. However, the internal audit team found that no groups or roles are identified as being responsible for the day-to-day management of each corporate risk. Informal ownership expectations exist; for example, the Information Technology Services Directorate is responsible for information technology related risks. However, there is no clear expectation to track, report or follow up on these risks.

"Organizations should consider specifying appropriate risk owners that have the accountability and authority to manage risks." (Treasury Board of Canada Secretariat, Guide to Integrated Risk Management)

"Organizations are encouraged to provide the risk owner(s) and related accountabilities, and these should be identified as individual(s) or role(s) but not a committee." (Treasury Board of Canada Secretariat, Guide to Corporate Risk Profiles)

The situation is similar for mitigation strategies that are developed annually by sectors and shared in the Integrated Business Plan. Offices of primary interest are designated for each deliverable contributing to mitigation strategies; however, no one is designated to

[3] The internal audit team noticed that the PSC started to implement controls regarding risk owners for the risk management process of 2023–24. However, the team wants to make sure that the recommendation is fully implemented and that risk owners track, report and follow up on risks.

measure or report on overall success, or to ensure the response is aligned with the risk appetite of senior management.

Causes

The internal audit team found that there has been no need to delegate risk ownership during the last 4 years since there has been no request for in-year reporting about the status of risk and the success of mitigation strategies. Stakeholders involved in the activities related to those risks are expected to act appropriately to reduce it to an acceptable level. This is not optimal when multiple directorates are involved in ensuring that mitigation actions are sufficient and aligned with the appetite of senior management.

Consequences

- The PSC does not know if risks are evolving and mitigated to an acceptable level for senior management (see section 3.3 Response to risks, for more information)
- Questions about risks and mitigation strategies are often left without specific answers during governance meetings, making the risk governance process less efficient

Recommendation 3

As part of the enterprise risk management framework, the Results and Delivery Division, in collaboration with the Executive Management Committee, should build a process to designate risk ownership for each specific risk and ensure accountability, including monitoring and ensuring a response aligned with the appetite of senior management.

3.3 Response to risks

There are no controls in place to measure the effectiveness of mitigation strategies. The risk appetite and risk tolerance are not clearly communicated; this does not support risk management and decision-making.

"Risk response **is the process of selecting and implementing measures to respond to a risk.** Typically, a general response strategy is selected (**accept** risk**, monitor** risk**, transfer** risk**, avoid** threat**, reduce** likelihood and/or impact of threat or **increase** likelihood and/or impact of opportunity**,** etc.). The organization's tolerance for risk should determine the type and extent of the response." (Treasury Board of Canada Secretariat, Guide to Integrated Risk Management)

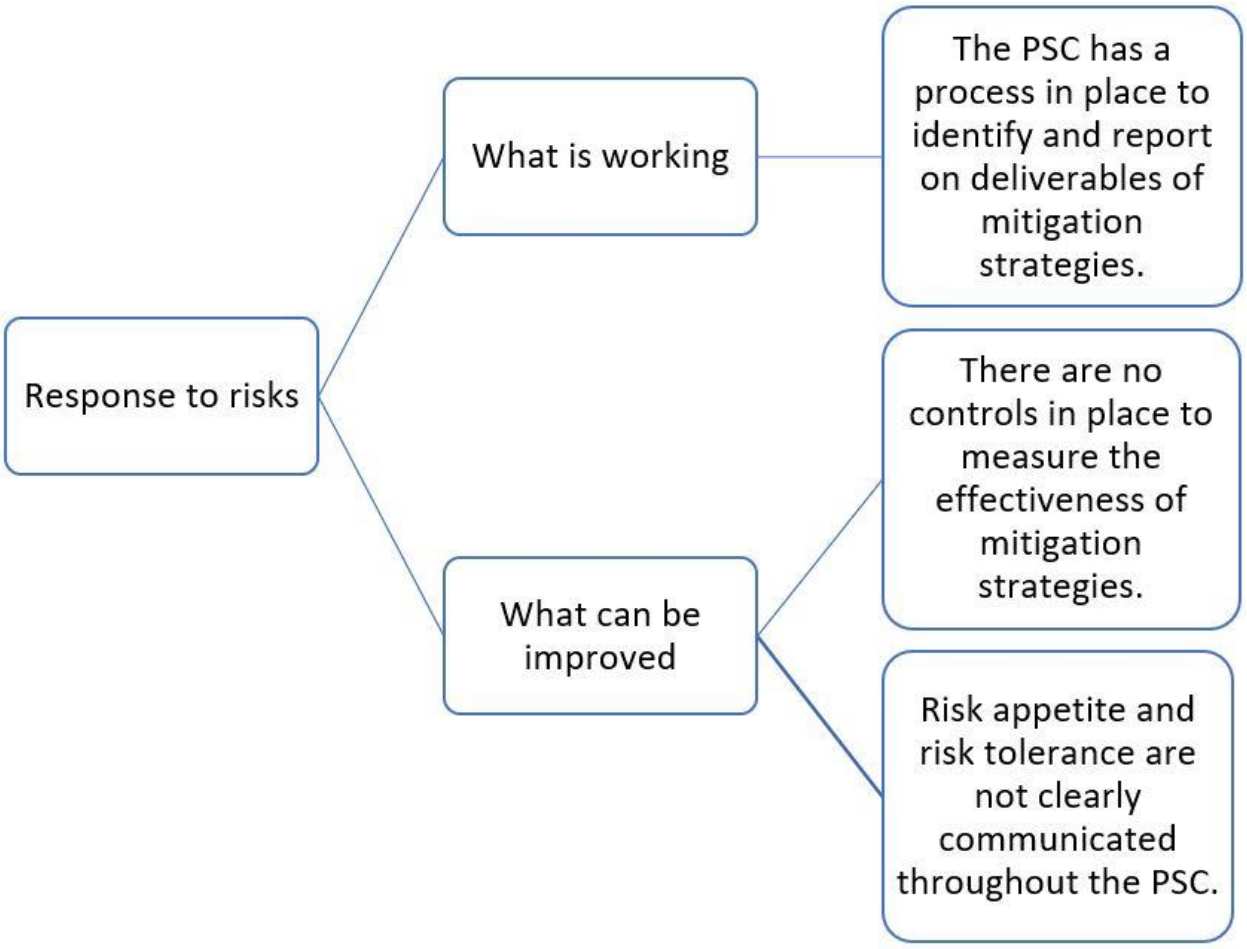
What we looked at and why it matters

The internal audit team assessed whether the PSC:

- has controls in place to ensure risk response is aligned with senior management's appetite
- measures the success of its strategies tomitigate risks to an acceptable level for senior management

When based on a clear understanding of senior management's risk appetite, the risk response helps to allocate the right amount of resources to specific actions, set the tone to measure success, and support the decision-making process.

Findings



Text version

This is a chart summarizing the findings of the Response to Risks section of the report.

The first box of the chart is titled "Response to Risks." Linked to this box are 2 boxes titled "What is working" and "What can be improved." Linked to the "What is working" box, another box presents this finding: "The PSC has a process in place to identify and report on deliverables of mitigation strategies." Linked to the "What can be improved" box, 2 other boxes present these findings: "There are no controls in place to measure the effectiveness of mitigation strategies" and "Risk appetite and risk tolerance are not clearly communicated throughout the PSC."

What is working

The PSC has a process in place to identify and report on deliverables of mitigation strategies.

Risk mitigation strategies are developed by each sector in collaboration with the Results and Delivery Division. This process begins with an annual call-out at the end of November from the Results and Delivery Division, requesting that sectors provide mitigation strategies and deliverables related to the previously identified corporate risks by the following January. The division assesses the mitigation strategies to determine if they are relevant for the coming year. Next, risk mitigation strategies are presented to sector management committees for feedback to help determine if the response corresponds to the nature and magnitude of the risk. Finally, mitigation strategies are presented for approval at the Executive Management Committee and then included in the coming year's Integrated Business Plan (see corporate risk management cycle graphic).

The execution of risk mitigation strategies and their associated deliverables are reported quarterly to the Resource Management Committee and the Executive Management Committee. Stakeholders can discuss the progress of the mitigation strategies and deliverables, but the time allocated to the discussion is short and insufficient as the members' attention is divided among many important topics.

What can be improved

There are no controls in place to measure the effectiveness of mitigation strategies.

The internal audit team found that there are no controls in place to measure the effectiveness of mitigation strategies. The quarterly updates presented to governance committees focus on the status of the deliverables, but their effectiveness in reducing risk is not assessed.

Causes

As risk ownership has not been delegated for the key corporate risks, no one is currently responsible for measuring the success of the mitigation strategies or ensuring alignment with the risk appetite of senior management.

Consequences

- There is a risk that not enough or too many financial and human resources are being allocated to the risk mitigation strategies

Most directors general who spoke about mitigation strategies during the interviews indicated that they did not have enough information about their success to support decision-making.

Recommendation

Recommendation 3 supports this finding.

Risk appetite and risk tolerance are not clearly communicated throughout the PSC.

The internal audit team found that the risk management process at the PSC does not allow for documenting and sharing risk tolerance and appetite. There is no clearly defined measure of success for mitigation strategies or acceptable level of risk that the PSC is willing to take. During interviews, directors general and vice-presidents expressed a willingness to take more calculated risks but were unsure about the overall appetite of senior management.

"Risk tolerance is the willingness of an organization to accept or reject a given level of residual risk. Risk tolerance may differ across the organization, based on the operating environment, stakeholders, etc., but must be clearly understood by the individuals making risk-related decisions on a given issue. Clarity on risk tolerance at all levels of the organization is necessary to support risk-informed decision-making and foster risk-informed approaches." (Treasury Board Secretariat, Guide to Integrated Risk Management)

"Risk appetite expresses the level of uncertainty an organisation is willing to take on in order to carry out its activities and realise its goals. Risk appetite should always lie within the organisation's tolerance limit to absorb risk. Risk tolerance may therefore be defined as the level of risk an organisation is able to absorb without significantly impacting the achievement of its strategic objectives." (Institute of Internal Auditors)

Causes

The internal audit team found no standardized process or mechanism to communicate the risk tolerance and appetite at the PSC. Tolerance is shared informally in discussions at various governance or bilateral meetings, and rarely documented.

"Several common approaches are used to communicate risk appetite. The first is to create an overall risk appetite statement that is broad enough yet descriptive enough for organizational units to manage their risks consistently within it. The second is to communicate risk appetite for each major class of organizational objectives. The third is to communicate risk appetite for different categories of risk." (Committee of Sponsoring Organizations of the Treadway Commission)

Consequences

- The understanding of risk tolerance and appetite varies across the PSC
- The PSC could miss opportunities that may have a positive impact on its mandate and reputation
    - Ten of the 15 senior managers interviewed thought that the PSC does not take enough risks
- The risk response may not be adequate for the PSC's needs and in line with the expectation of senior management

Recommendation 4

The Results and Delivery Division, in collaboration with the Executive Management Committee, should ensure that the enterprise risk management framework includes a process to clearly identify and communicate the Executive Management Committee's risk tolerance and appetite to PSC employees.

3.4 Tools

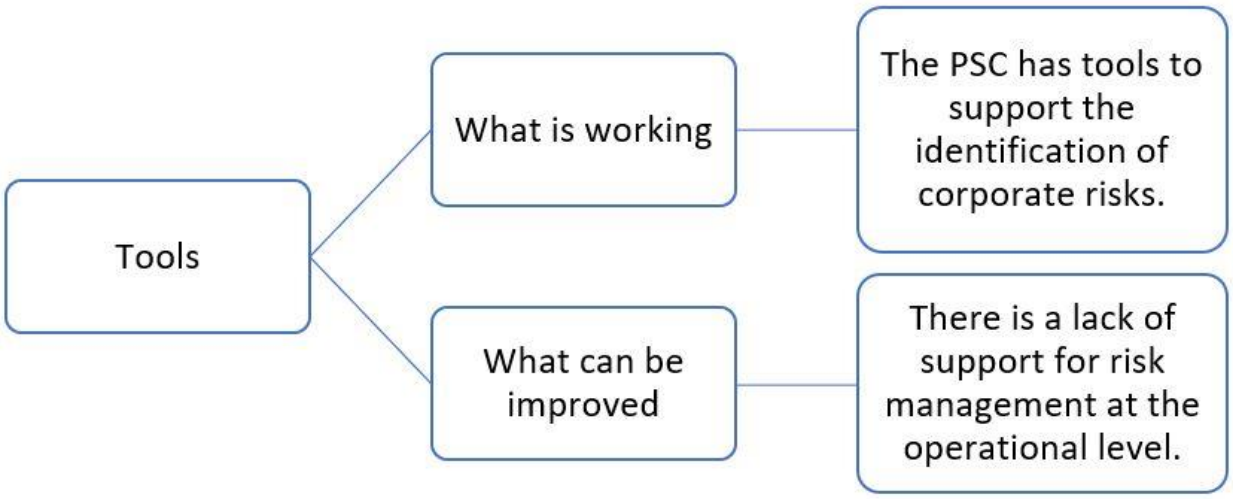
The lack of support for risk management at the operational level does not promote risk management and sound decision-making.

What we looked at and why it matters

The internal audit team assessed whether the PSC has the tools and expertise to support good risk management practices across the organization. In its *Guide to Integrated Risk Management*, the Treasury Board of Canada Secretariat expects organizations to have the capacity and tools to foster a risk-informed culture applicable at different levels of an organization, including programs and projects. The analysis took into consideration

the size of the PSC, the nature of its activities and requirements based on the risk management practices in place.

Findings



Text version

This is a chart summarizing the findings of the Tools section of the report.

The first box of the chart is titled "Tools." Linked to this box are 2 boxes titled "What is working" and "What can be improved." Linked to the "What is working" box, another box presents this finding: "The PSC has tools to support the identification of corporate risks." Linked to the "What can be improved" box, another box presents this finding: "There is a lack of support for risk management at the operational level."

What is working

The PSC has tools to support the identification of corporate risks.

The internal audit team found that for the corporate risk identification process that occurs in the fall, the Results and Delivery Division has developed and shared tools to support this process and leveraged Treasury Board of Canada Secretariat guides. For example, during the cyclical risk identification process, the *Guide to Risk Statements* and other key documents are shared with stakeholders. The participants who took part in the risk identification exercises during the last 4 years have received various versions of those documents to support them in the process.

What can be improved

There is a lack of support for risk management at the operational level.

The internal audit team assessed the risk management practices of the GC Jobs Transformation project, the Second Language Evaluation – Unsupervised Testing Project and the Priority Entitlement Program. All 3 were found to have developed risk management practices, processes, tools and documentation. The internal audit team found that as there was little support across the PSC, including expertise and tools, these practices were developed on an ad hoc basis, relying on team members' knowledge of risk management. Many interviewees (not only from the sample projects teams) mentioned they could benefit from more support, for example in terms of training, and that they rely on their own limited skills.

Causes

The responsibility for supporting good risk management practices has not been clearly assigned at the PSC. The expectation is that the Results and Delivery Division will provide support for identifying corporate risk, but no one is in charge of advertising training, promoting tools or raising awareness about risk management practices. For example, the Canadian School of Public Service offers several courses for federal public servants. The courses cover different components of risk management, from a general introduction to risk management to identifying, assessing and responding effectively to risks. The Treasury Board of Canada Secretariat also has tools to help manage risks. However, the internal audit team found that these training courses and tools are not shared with PSC employees through the PSC learning catalogue, workplace tools on Intracom or the *PSC Express*.

Consequences

- Due to a lack of support, issues similar to those found for corporate risk management are observed at the operational level, including:
    - a lack of consistency among risk identification processes
    - issues are sometimes categorized as risks
    - a lack of clear risk response
    - no controls to measure the effectiveness of mitigation strategies
- There is some duplication of effort and a lack of consistency when each team is responsible for developing its own risk management tools
- The effectiveness of risk management practices relies on the knowledge of key employees

Recommendation 5

The Vice-President of the Corporate Affairs Sector should identify a group that will be responsible for promoting tools and training to support an organizational-wide risk management culture.

4. Conclusion

Sound risk management practices are essential to informed decision-making and to achieving organizational objectives.

These practices do not support risk management and sound decision-making:

- the risk identification process fails to identify important corporate risks and support in-year updates
    - Risk rating[4]: High
- some identified corporate risks are issues
    - Risk rating: High
- corporate risk ownership for day-to-day management is not clearly delegated
    - Risk rating: High
- there are no controls in place to measure the effectiveness of mitigation strategies
    - Risk rating: High
- risk appetite and risk tolerance are not clearly communicated throughout the PSC
    - Risk rating: High
- there is a lack of support for risk management at the operational level
    - Risk rating: Medium

As a result of the audit findings, this audit concludes that risk management practices at the PSC are insufficient to support sound management and decision-making and that improvements are required to support good risk management practices.

[4] The risk rating describes the level of impact and likelihood (combined) that risk management practices will not support sound public management and informed decision-making if the recommendations are not taken into consideration. A “high” risk rating means that the internal audit team expects prompt implementation of the action plan following the recommendation. Implementation of recommendations should be prioritized based on the risk rating.

The PSC would benefit from implementing a formalized risk enterprise management framework, tailored to its size and activities, to increase the effectiveness of its practices and provide a clearer direction to all staff about how risks should be reported and managed. Other possible improvements include:

- ensuring enough time in-year for discussion about risks and risk response
- separating issues from risks in the various reports (Departmental Plan, Integrated Business Plan and quarterly reports).
- ensuring proper risk ownership and responsibility for aligning the risk response with the appetite of senior management
- communicating the risk tolerance and appetite of senior management
- promoting tools and training to support a risk management culture across the PSC

Implementing the recommendations will lead to improved risk management practices and will benefit the PSC by:

- providing greater awareness of PSC risks and reducing the chance they become issues
- promoting calculated risk-taking to achieve objectives
- supporting the efficient use of resources, by reducing the risk of allocating too much or not enough resources to risk responses and mitigation strategies
- coordinating efforts for developing tools and risk management practices across the PSC

Annex A: Audit findings and recommendations

Findings

What is working

- The PSC has a process to identify and communicate key corporate risks.
- Roles and responsibilities are well defined within the governance structure of the PSC for the corporate risk identification process.
- The PSC has a process in place to identify and report on deliverables of mitigation strategies.
- The PSC has tools to support the identification of corporate risks.

What can be improved

- The risk identification process fails to identify important risk and support in-year updates. (Recommendation 1)
- Some identified corporate risks are issues. (Recommendation 2)
- Corporate risks ownership for the day-to-day management is not clearly delegated. (Recommendation 3)
- There are no controls in place to measure the effectiveness of mitigation strategies. (Recommendation 3)
- Risk appetite and risk tolerance are not clearly communicated throughout the PSC. (Recommendation 4)
- There is a lack of support for risk management at the operational level. (Recommendation 5)

Recommendations

- The Vice-President of the Corporate Affairs Sector, in collaboration with the Executive Management Committee, should implement an enterprise risk management framework that includes a clear process to identify, track and update key corporate risks. They should also ensure that enough time is allocated to identify and discuss risks.
- The Results and Delivery Division, in collaboration with the Executive Management Committee, should include a list of key issues and action plans in the planning process, separate from the risks and mitigation strategies list.
- As part of the enterprise risk management framework, the Results and Delivery Division, in collaboration with the Executive Management Committee, should build a process to designate risk ownership for each specific risk and ensure accountability, including monitoring and ensuring a response aligned with the appetite of senior management.
- The Results and Delivery Division, in collaboration with the Executive Management Committee, should ensure that the enterprise risk management framework includes a process to clearly identify and communicate the Executive Management Committee's risk tolerance and appetite to PSC employees.
- The Vice-President of the Corporate Affairs Sector should identify a group that will be responsible for promoting available tools and training to support an organizational wide risk management culture.

Annex B: Audit criteria

1. The PSC has an integrated risk management process that supports decision-making

1.1 There is a process to identify organization-wide risks in a timely manner.

- The PSC has a process to identify and communicate its key corporate risks. However, it is not effective to identify emerging risks and to ensure proper risk oversight.

1.2 Mitigation strategies and controls are developed and implemented to address risks.

- The PSC has a process to identify deliverables as mitigation strategies. However, there are no controls in place to measure the effectiveness of these strategies.

1.3 Risks and mitigation strategies are monitored, reassessed and communicated to all governance levels of the organization to support decision-making.

- The PSC has a process to report on deliverables of the mitigation strategies. However, the process fails to support in-year updates regarding risks and reassessment of the mitigation strategies.

2. The governance supports good risk management practices

2.1 The PSC has adequate and effective risk management governance, including roles, responsibilities and accountabilities.

- Roles and responsibilities are well defined within the governance structure of the PSC. However, risk ownership is not clearly identified for corporate risks, and no stakeholders are clearly held accountable for the success of the risk mitigation strategies.

2.2 Risk management practices are aligned with the level of tolerance expected and communicated by senior management.

- The risk management process at the PSC does not allow for documenting and sharing risk tolerance and appetite evenly among senior management.

2.3 The PSC has tools and the expertise to support good risk management practices.

- The Results and Delivery Division has developed tools to support the identification of corporate risks and leveraged Treasury Board of Canada Secretariat guides when necessary. However, there is a lack of support for risk management at the operational level to promote good risk management practices.

Annex C: Management Response and Action Plan

Recommendation 1:

The Vice-President of the Corporate Affairs Sector, in collaboration with the Executive Management Committee, should implement an enterprise risk management framework that includes a clear process to identify, track and update key corporate risks. They should also ensure that enough time is allocated to identify and discuss risks.

Risk level associated with not addressing recommendation: High

Response: The Vice-President of the Corporate Affairs Sector supports the recommendation to adopt an enterprise risk management framework. Risk management is a critical component of the integrated planning approach, through regular engagement with sectors, directorates and the PSC.

Planned actions: An enterprise risk management framework will be developed in line with the Treasury Board of Canada Secretariat's risk management framework. The framework will include a process to ensure quarterly monitoring as well as regular discussions at governance committees.

Timelines: Q3 2023–24

Office of Primary Interest: Corporate Affairs Sector

Recommendation 2

The Results and Delivery Division should include a list of key issues and action plans in the planning process, separate from the risks and mitigation strategies list.

Risk level associated with not addressing recommendation: High

Response: The Vice-President of the Corporate Affairs Sector supports the recommendation.

Planned actions:

- As part of the integrated planning approach, regular meetings with sectors and directorates will allow for identification of key issues and action plans.
- As part of the integrated planning approach, sectors and the Executive Management Committee will be provided with key issues, risk, and risk responses and/or mitigation strategies for review and discussion.

Timelines:

Action 1: Q2 2023–24
Action 2: Ongoing as per planning timelines.

Office of Primary Interest: Corporate Affairs Sector, Finance and Corporate Planning Directorate, and Results and Delivery Division

Recommendation 3

As part of the enterprise risk management framework, the Results and Delivery Division, in collaboration with the Executive Management Committee, should build a process to designate risk ownership for each specific risk and ensure accountability, including monitoring and ensuring a response aligned with the appetite of senior management.

Risk level associated with not addressing recommendation: High

Response: The Vice-President of the Corporate Affairs Sector supports the recommendation.

- Planned actions: Roles and responsibilities of risk owners will be clearly identified as part of the risk framework.

Timelines: Q3 2023–24

Office of Primary Interest: Corporate Affairs Sector, Finance and Corporate Planning Directorate, and Results and Delivery Division

Recommendation 4

The Results and Delivery Division, in collaboration with the Executive Management Committee, should ensure that the enterprise risk management framework includes a

process to clearly identify and communicate the Executive Management Committee's risk tolerance and appetite to PSC employees.

Risk level associated with not addressing recommendation: High

Response: The Vice-President of the Corporate Affairs Sector agrees that an enterprise risk management framework should include a communication strategy to inform PSC employees.

Planned actions:

- Develop a communications plan in collaboration with the communications team to ensure the most effective way to inform PSC employees about senior management's risk tolerance.
- The Results and Delivery Division, in collaboration with Communications and Parliamentary Affairs Directorate, will develop an Intracom page containing planning, reporting, risk and performance measurement information.

Timelines:

Action 1: Q2 2023–24
Action 2: Q3 2023–24

Office of Primary Interest: Corporate Affairs Sector

Recommendation 5

The Vice-President of the Corporate Affairs Sector should identify a group that will be responsible for promoting available tools and training to support a risk management culture.

Risk level associated with not addressing recommendation: Medium

Response: The Vice-President of the Corporate Affairs Sector agrees with the recommendation.

Planned actions:

- The Results and Delivery Division will be responsible for promoting available tools and training to support a risk management culture.
- The Results and Delivery Division will collaborate with the Human Resources, Workplace and Security Directorate to include relevant risk training in the PSC's learning catalogue.

Timelines:

Action 1: Q2 2023–24
Action 2: Q3 2023–24

Office of Primary Interest: Corporate Affairs Sector