Employment and Social Development Canada
Emploi et Développement social Canada

Canada

Unclassified

Audit of Risk Management Practices

November 2018

Internal Audit Services Branch

Audit of Risk Management Practices

This publication is available for download at canada.ca/publicentre-ESDC .
It is also available upon request in multiple formats (large print, MP3, Braille, audio CD, e-text CD, DAISY or accessible PDF), by contacting 1 800 O-Canada (1-800-622-6232).
By teletypewriter (TTY), call 1-800-926-9105.

PDF
Cat. No. : Em20-116/2019E-PDF
ISBN: 978-0-660-29194-9

ESDC
Cat. No. : SP-1194-01-19E

TABLE OF CONTENTS

1. BACKGROUND

1.1 Context

In a dynamic and complex environment, organizations are required to manage risks so that they reduce their threats to an acceptable level and exploit their potential as much as possible. Risk management involves establishing processes and practices for identifying, assessing, mitigating, monitoring and reporting on risks for the successful achievement of organizational objectives.

The Government of Canada is committed to strengthening risk management practices in the public service to promote sound decision-making and accountability. As such, Treasury Board (TB) developed the Framework for the Management of Risk (the Framework), effective August 2010.

The Framework provides principles and guidance for senior management to consider in their efforts to establish sound risk management practices in their organization. According to the Framework, effective risk management would enable senior management to:

- Identify and explain different types of risks at all levels of their organization and how they can be managed;
- Provide guidance on setting risk tolerance levels and making decisions informed by considerations of risk and mitigation strategies;
- Support learning opportunities in their organization, including formal and informal risk management practices that respond to the needs and culture of their organization;
- Lead by example through embedding risk management principles and practices in the management of their organization; and
- Align their risk management practices with TB management practices and policies.

Within Employment and Social Development Canada (ESDC), the Strategic and Service Policy Branch (SSPB)[1] leads the Department's corporate risk and environmental scan processes. In addition, SSPB prepares Corporate Risk Profile (CRP) updates, communicates and implements the departmental Integrated Risk Management (IRM) Strategy and performs appropriate follow-up.

[1] http://esdc.prv/en/sspb/corporate/index.shtml#s1

1.2 Audit Objective

The objective of this audit was to provide assurance to senior management that ESDC's risk management framework and practices were adequate, functioned as intended and supported informed decision-making.

1.3 Scope

The scope of this audit included key departmental structures, processes and practices pertaining to risk management and the development of the CRP.

In addition to audit activities at National Headquarters, regional visits were conducted in all four ESDC regions to review existing risk management practices and determine the level of adherence to national standards across geographic areas.

1.4 Methodology

The audit was conducted using a number of methodologies including:

- Documentation review and analysis;
- Interviews with management and staff from SSPB;
- Interviews with management and staff from branches and regions;
- File reviews; and
- Information analysis and validation to support the conclusions.

2. Audit Findings

2.1 Risk Governance could be improved

ESDC is a large, complex, and geographically diverse organization. Departmental programs are generally managed across several branches and regions to deliver services to Canadians. Risks at the branch and regional levels are managed by teams within these organizations and corporate risks are managed by the risk owners at the Assistant Deputy Minister (ADM) level. The SSPB facilitates the Enterprise Risk Management (ERM) process for ESDC.

We expected to find a governance structure that oversees departmental risk management practices, including clearly defined and communicated roles and responsibilities.

We found that roles and responsibilities of the main stakeholders involved in the risk management are clearly defined in the departmental IRM Framework and in the CRP. For example, the CRP specifies that the Deputy Minister is responsible for effective risk management practices department-wide. ADM and their executive committees are responsible for managing risks to programs, services, projects and business lines within their branches or regions. Those responsibilities include having sufficient capacity and competency for effective risk management. Executives and managers are in charge of putting into practice the risk management process, and communicating key risks to the appropriate governance and oversight committees within their respective branches or regions.

Interviews noted that the majority of risk planners within branches and regions clearly understand their roles and responsibilities as well as the division of responsibility between SSPB and branches/regions. These include branches' and regions' responsibilities in establishing and updating their quarterly Branch Risk Register (BRR) and SSPB's role in preparing and updating the CRP.

ESDC's IRM Framework as well as the CRP outline multiple committees that oversee departmental risk management practices. We found these committees don't challenge the risk information reported in the CRP. We also found that branches and regions consistently provide their risk information to SSPB. While SSPB provides advice and guidance to branches and regions in the development of risk statements and mitigation strategies, the challenge function is minimal in either challenging the risks reported in the BRRs or validating that mitigation strategies outlined in the CRP are being implemented as intended. We noted that SSPB has limited capacity within the corporate risk team to provide a challenge function to validate that risks identified in BRRs reflect relevant information in the internal and external departmental environments. In fact, during the audit, the corporate risk function had the equivalent of 1.5 full time employees responsible for all corporate risk activities, including training.

According to risk management literature reviewed, most successful organizations have a strong risk function with a clear mandate to:

- Obtain and develop the required resources and capacities;
- Promote the importance of risk management to the organization;
- Involve those that need to be involved and hold them accountable; and
- Provide expertise and a robust challenge function.

In our opinion, strengthening the challenge function in SSPB would allow ESDC to improve risk governance and further mature risk management within the organization. This area of improvement should be addressed when updating the IRM Framework (refer to recommendation 1).

2.2 ESDC's Integrated Risk Management Framework could be enhanced

Corporate Planning and Management Directorate within SSPB has developed a departmental IRM Framework which contains the following key elements:

- Roles and responsibilities;
- Definitions, terminology and taxonomy;
- Risk management process;
- Integration of risk management;
- Communications; and
- Monitoring and reporting processes.

We reviewed ESDC's IRM Framework and identified areas for improvement. For example, we noted that the IRM Framework was not formally approved and has been in draft format since 2015. Some content refers to the outdated 2013 version of Committee of Sponsoring Organizations of the Treadway Commission, and there are inaccuracies and a lack of clarity within the IRM Framework. For instance, the risk assessment section confuses risk management tools and methodologies to identify risk with documents where risks are listed. The IRM Framework also mixes the concepts of imminence/proximity of the risk with the likelihood of occurrence. Furthermore, interviews indicated that the IRM Framework was not widely communicated.

An updated, enhanced, approved, and widely disseminated IRM Framework is an important element of sound risk management. It would enable a standardized and systematic approach to risk management throughout the Department, and help build and maintain stronger practices which will inform decision-making and priority-setting.

Recommendation

1. SSPB should review and update the IRM Framework, and formally issue it to all stakeholders involved in the risk management process.

Management Response

Management agrees. SSPB will update the integrated ERM Framework with up to date risk literature and concepts (methodology and definitions, including tolerance). Based on the outcome of Recommendation 3, the IRM Framework will be updated with the Governance, as well as any changes to processes, roles and responsibilities, including the challenge function. Actions are expected to be completed by June 2019.

2.3 ESDC's Risk Management Practices could be strengthened

Risk Management Process

ESDC's risk management process begins with a call letter from the Senior ADM of SSPB to all of the ADMs requesting quarterly updates of their BRR, environmental scan, and accompanying documents. The corporate planning teams within all branches and regions, in collaboration with their directorates and/or business lines, update the BRR templates and table them for discussion at their respective executive committees. Finally, the planning teams compile the updates and send the completed documents to their ADMs for final review and approval before submitting them to SSPB. Information gathered during the quarterly BRR updates is used to inform the establishment of the CRP.

Our review showed that SSPB has made significant progress to improve and standardize the process throughout the Department by developing guidelines, training, tools and templates. Some improvements are needed in the areas of risk statements, integration of the risk management process with the planning cycle, oversight of risk identification and assessment, and risk treatment. These areas are further discussed below.

Risk Tolerances

We expected that discussions around risk tolerances would take place throughout the risk management cycle to help staff understand the range of risk levels within which they are expected to operate in pursuit of the achievement of ESDC's objectives. Hence allowing risk management stakeholders to determine whether a given risk should be accepted, mitigated, or avoided.

We found that there are discussions regarding the level of risk that necessitates mitigating actions during the quarterly BRR update as well as during the development of the CRP. The IRM Framework also provides key concepts and principles related to risk tolerance. Furthermore, during the audit we were told that the Department was in the process of establishing fraud risk assessments for key programs which may generate data that could be leveraged to develop risk tolerances.

The audit team encourages ESDC to continue and expand discussions around risk tolerances and incorporate them into departmental risk management practices.

Risk Statements

We expected that risk statements would include and outline the risk event, the potential driver(s) of the event, and the consequences if the risk materializes.

We assessed risk statements in the CRP and BRRs, and we noted that risk statements are often too general and don't target a precise and specific event. Sometimes risks are stated as issues, objectives, controls and/or mitigating strategies. In our file review of 238 risk statements, the audit team found that 120 (50%) met the definition of a true risk statement outlined above. In our review of the CRP we found that none of the nine risk statements met the true definition of a risk statement.

Clear, concise and well-articulated risk statements are fundamental for sound risk management. They would facilitate communication and common understanding of risks facing ESDC, help senior management understand the risk drivers and how these impact the achievement of the Department's objectives. It would also assist in the allocation and use of resources through the development of more precise and targeted mitigation actions.

The implementation of recommendations 1, 3, and 4 would, in our opinion, address the issues related to risk statements highlighted in this section.

Integration of Risk Management Process with the Planning Cycle

We expected that risks identified in the CRP would be linked to relevant ESDC strategic objectives, and risks identified in the BRRs would be linked to branches' and regions' strategic objectives.

ESDC 2017-18 Calendar for the Corporate Planning and Reporting Process incorporates risk management (corporate environmental scan, BRRs and CRP) into the departmental planning cycle. However, our review of the CRP showed that departmental risks are not always explicitly linked to ESDC's strategic objectives. We also noted that the development of the CRP is not fully integrated with the departmental planning cycle. For example, the 2017-18 CRP was approved in January 2018 towards the end of the fiscal year, compared to the corporate planning cycle which typically takes place at the beginning of the fiscal year.

At the branch and regional levels, activities are underway to align risk management with the planning cycle. Most branches and regions have integrated their risk functions with their planning unit to reduce duplication of efforts and, in some cases, better tie risks to the achievement of branches' or regions' objectives. The results of our review showed that 42% of ESDC branches and regions have some linkages between the risks identified in their BRRs and their strategic objectives.

In our opinion, fully integrating risk management practices into the departmental planning cycle could contribute to the achievement of strategic objectives by facilitating informed decision-making and more efficient use of resources.

Recommendation

2. SSPB, in collaboration with appropriate stakeholders, should fully integrate the risk management process into the departmental planning cycle.

Management Response

Management agrees. SSPB recognizes the need to better integrate the risk management process into the departmental planning cycle. Actions are expected to be completed by July 2019.

Risk Identification and Assessment

At the branch and regional levels, risks are identified through discussions at various meetings and committees, and review of risk documentation such as Privacy Impact Assessments, Business Impact Analysis, Memorandum to Cabinet, Treasury Board Submissions. Most branches also perform a quarterly environmental scan which includes threats and opportunities and takes into account both internal and external factors.

Interviews revealed that the conduct of quarterly environmental scans has increased risk management discussions at all levels and helped advance risk management awareness and knowledge. The audit identified some opportunities to improve the risk management process at both the corporate and branch/regional levels going forward. We found the process lacks a formal, documented and repeatable methodology to identify key risks that could impede the achievement of strategic objectives, and to assess the impact and likelihood of risks that have been identified. We also noted limited use of data as evidence to support the risk identification and assessment processes. As a result, risks are identified and assessed based on the experience and professional judgement of those who provide input to the CRP and BRRs.

We observed that risk identification and assessment practices vary widely across ESDC. In some branches and regions the process is well developed and established, while for others the process is at an earlier stage. Some branches and regions have dedicated resources and structures in place to support a rigorous process for identifying and assessing risks, while others see it as a paper exercise and a tick box. We have been told by those with a rigorous process that a key contributing factor to their success is support from their senior management.

We also noted inconsistencies in the depth and robustness of the risk identification and assessment processes within branches and regions.

Risk Treatment

Mitigation actions are documented in the CRP for all identified corporate risks, and they are documented in BRRs for identified risks at the branch and regional levels. Corporate mitigation actions documented in the CRP include key risk drivers to be mitigated, Office of Primary Interest (OPI) at the branch level, status, as well as planned completion dates. Key information provided in mitigating actions in the BRRs include status of the mitigating activities and the expected completion dates. Key weaknesses were noted in the mitigating actions outlined in both the CRP and BRRs. For example, mitigation actions were neither specific nor documented as a list of precise executable actions to be undertaken in order to bring the identified risks to an acceptable level. In addition, for the CRP, the OPIs were identified at branches' and regions' level with no specific individual or position owning the risk nor responsible for validating that risk responses are implemented and effective. Most BRRs don't outline the OPI or the risk owner, which create some confusion around the accountability of risk owners and the execution of mitigating actions. Such a situation is partially due to departmental guidance and tools not requiring explicit identification of the risk owners.

In addition, for both the CRP and BRR, there is no evidence that performance measures have been developed nor implemented to assess whether mitigating actions are in place and having the desired effect. The audit team reviewed a random sample of two mitigation actions from each of the 19 BRRs. Of the 38 mitigation actions reviewed, we found three contained sufficient information about the mitigation actions, five could be improved, and 30 were deemed not adequate.

In our opinion, it is important that mitigation actions be developed and documented in a way that provides sufficient detail about what specific tasks are to be undertaken, particularly, when, where, how often, and by whom. Clear accountability for implementing mitigation actions and explicit measurement need to be defined to validate that a specific risk treatment is implemented and that it has had the intended effect on reducing the level of risk.

Recommendation

3. SSPB should develop and implement:

    a. An oversight mechanism to confirm the adequacy of risk identification, assessment, and mitigation actions.

    b. A monitoring mechanism to ascertain that mitigation actions have been executed.

Management Response

Management agrees. SSPB will propose options for an oversight mechanism within the existing ESDC Risk Governance structure to increase the adequacy and accountability for risk identification, assessment and treatment. SSPB will also take the lead in developing mechanisms to monitor risk mitigation strategies implementation. Actions are expected to be completed by May 2019.

Branch Risk Registers

The BRR review found that 95% of branches and regions submitted an updated and approved BRR. Branches and regions document their risks for the quarter using the prescribed template, which includes risk categories (e.g. human resources, strategic, etc.), risk statements, risk ratings (low, medium or high), mitigation actions and target implementation timelines.

The audit team noted that all branches and regions submitted their quarterly updates signed off at the ADM level. SSPB has also introduced an ADM Attestation Form. The signed form confirms that the risk information under the ADM's responsibility is accurate and ready to be presented to the Portfolio Management Board (PMB), other governance bodies and can be shared with ESDC employees.

Interviews and documentation review suggested that monitoring and reporting of branch and regional risks would benefit from requiring that the following information be provided in the BRR template:

- Linking risks to objectives;
- Linking risks to programs;
- Likelihood and impact of risks;
- Risk owners;
- Risk trends over time; and
- Tracking new and removed risks in BRRs.

Internal Audit encourages SSPB to update the BRR template to require the above-mentioned information be provided. By doing so, the quality of information gathered to prepare the CRP will be enhanced.

Corporate Risk Profile

According to TB guidance, the CRP serves as a forward looking medium to describe the organization's key risks which affect the achievement of its strategic objectives. The CRP is to be developed in a balanced way with enough detail to provide context and a clear description of how risks are identified, analysed, assessed, treated and reported but it

shouldn't overwhelm the reader with detailed information not useful for effective decision-making.

We reviewed ESDC's CRP and found that it presents a consolidated view of key departmental risks on an annual basis. But the CRP does not contain regulatory risks. We also noted that the links between the risks and ESDC's objectives are not clearly outlined. We were informed during the interviews that the structure, volume and quantity of information in the CRP make it very wordy and cumbersome to understand and use.

The completed CRP is tabled at PMB annually for discussion. The CRP for 2017-18 was only approved in January 2018. Some interviewees suggested that the CRP should be better integrated into the planning cycle, be prepared well in advance of the beginning of the fiscal year and shared with key stakeholders ahead of time to allow for discussion and comments before approval.

Internal Audit encourages the Department to review whether regulatory risks should be included in the CRP. The implementation of recommendations 1, 2, 3 and 4 would, in our opinion, help resolve the remaining CRP issues outlined above.

2.4 Training could be enhanced

SSPB has made efforts to continuously improve risk management practices, raise awareness and facilitate consistency across the Department through the following:

- Developing and providing training;
- Developing and updating templates;
- Creating working groups; and
- Sharing information and best practices among risk management practitioners.

SSPB developed and delivered three non-mandatory risk training courses in the summer of 2017. Four training sessions have been offered to date. We were informed that 89 employees have taken some training, and 16 out of 19 branches and regions have sent at least one employee to attend a risk management training course.

Our review showed that the training material covers key concepts such as the definition of risk, its lifecycle, ERM, and the distinction between issues and risks. We noted that the training is not designed to target any specific group or function, rather the training is aimed at a variety of roles and responsibilities, levels, and types of work.

Interviews with staff and management involved in risk management indicated that they view training as a step in the right direction. Interviews also revealed that some individuals were unaware that departmental training was available while others who have taken the training indicated that more tailored and practical training with real examples and case studies would be more useful.

In discussions with risk management practitioners across the Department, we noted a consistent desire to learn and improve, as well as a willingness to adopt more advanced risk management practices. Certain branches and regions have proactively made improvements to departmental templates and tools in order to provide more useful information to senior management while continuing to provide the required quarterly updates. Some regions took the initiative to send their employees to attend external risk management training at local universities.

Recommendation

4. SSPB should review departmental risk management training to ensure it is tailored to the levels and types of risk work performed throughout the Department.

Management Response

Management agrees. SSPB will evaluate existing training in ESDC and Canada School of Public Service to identify and tailor training that addresses the needs of the various levels and types of risk work performed in the Department. SSPB will also ensure that the completed risk training curriculum is available to target groups. Actions are expected to be completed by December 2019.

3. Conclusion

The audit concluded that ESDC's risk management framework and practices are aligned with TB principles and guidance. All fundamental elements outlined in the TB Framework for the Management of Risk are in place in ESDC.

The audit also concluded that key elements of ESDC's risk management framework and practices are adequate and working as intended. These elements include roles and responsibilities, risk tolerance, risk identification and risk categories.

Other elements need to be enhanced in order to further improve the maturity of ESDC's risk management and better inform decision-making. These elements include integrating the risk management process with the departmental planning cycle, and providing for proper oversight of the identification, assessment and mitigation of risks.

4. Statement of Assurance

In our professional judgement, sufficient and appropriate audit procedures were performed and evidence gathered to support the accuracy of the conclusions reached and contained in this report. The conclusions were based on observations and analyses at the time of our audit. The conclusions are applicable only for the audit of Risk Management Practices. The evidence was gathered in accordance with the Treasury Board *Policy on Internal Audit* and the *International Standards for the Professional Practice of Internal Auditing*.

APPENDIX A: AUDIT CRITERIA ASSESSMENT

Audit Criteria		Rating
It was expected that the Department has established a governance structure to oversee departmental risk management practices and facilitate consistency within the organization.		Controlled, but should be strengthened; medium-risk exposure
It was expected that the Department has clearly defined and communicated:	roles, responsibilities related to risk management	Sufficiently controlled; low-risk exposure
	accountabilities related to risk management	Controlled, but should be strengthened; medium-risk exposure
It was expected that the Department has developed and maintains guidance, guidelines, training and tools that are relevant, understandable, and aligned with TB requirements.		Controlled, but should be strengthened; medium-risk exposure
It was expected that ESDC has established a process to identify, assess, prioritize, respond, monitor and report on risk.		Controlled, but should be strengthened; medium-risk exposure
It was expected that departmental risk management methodologies, approaches, directives, training and tools are consistently applied across branches.		Controlled, but should be strengthened; medium-risk exposure
It was expected that appropriate measures are in place to monitor risk trends and risk treatment strategies.		Controlled, but should be strengthened; medium-risk exposure
It was expected that feedback and review mechanisms are used to leverage lessons learned from managed risks, risk failures and/or, near misses to improve ESDC's risk management process.		Controlled, but should be strengthened; medium-risk exposure

APPENDIX B: GLOSSARY

ADM	Assistant Deputy Minister
BRR	Branch Risk Register
CRP	Corporate Risk Profile
ERM	Enterprise Risk Management
ESDC	Employment and Social Development Canada
IRM	Integrated Risk Management
OPI	Office of Primary Interest
PMB	Portfolio Management Board
SSPB	Strategic and Service Policy Branch
TB	Treasury Board