Public Safety Canada | Sécurité publique Canada

Public Safety Canada
Internal Audit of Integrated Risk Management

APPROVED

September 2013
RDIMS #893596

Canada

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

The Department identified integrated risk management (IRM) as an area that should be audited in 2013, as part of the annual risk-based audit planning process. The rationale for this decision was also supported as IRM was identified as one of the department's management priorities in 2013. Public Safety Canada (PS) has never audited IRM.

Risk management makes a significant contribution in strengthening departmental capacity to recognize, understand, accommodate and capitalize on new challenges and opportunities. It prepares an organization to respond to change and uncertainty and enables more effective decision-making.

International standards[1] and government-wide expectations of good governance emphasize that all types of risks should be considered and integrated in all planning and delivery activities, at the strategic and operational levels. The Treasury Board (TB) *Framework on the Management of Risk* provides guidance to Deputy Heads on the implementation of effective risk management practices at all levels of their organization. This Framework supports strategic priority setting and resource allocation, informed decisions with respect to risk tolerance, and improved results.

The *Management Accountability Framework* (MAF) which is a key performance management tool for the federal government also expects departments to incorporate risk management practices and principles into the organization's strategic, operational and functional activities.

In 2010 PS approved an Integrated Risk Management Policy and in 2013 updated the Integrated Risk Management Framework. This framework is designed to communicate PS's risk management strategy to all levels of staff, and supply the means to build and maintain a strong risk management capacity.

Audit Objective

The objective of this audit was to provide reasonable assurance that the department's approach to integrated risk management was adequate and effective to ensure a consistent approach was used and that risk information was appropriately integrated into decision making. The audit covered the period of September 1, 2011 to December 31, 2012.

Summary of Findings

The audit found a well-defined and appropriately communicated PS *Integrated Risk Management Policy* (IRM Policy), and PS *Integrated Risk Management Framework* (IRM Framework). Both documents had identifiable objectives, clear roles and responsibilities, and reporting timeframes which were aligned with the TB *Framework for the Management of Risk* and TB *Guide to Integrated Risk Management*.

[1] ISO 31000 Risk Management Principles and Guidelines

While there are mechanisms to monitor the implementation of the Policy, they remain periodic and at a high-level. There are no mechanisms that identify timely information on the state of implementation of risk management and the associated training gaps. The audit recognizes that the Strategic Policy Branch (SPB) has succeeded in putting in place many foundational elements with very few resources; however a few select indicators to support monitoring would ensure that the momentum gained is not lost.

At the departmental level, the Corporate Risk Profile (CRP) captures the high-level strategic risks. PS has received strong MAF ratings for this tool's development and implementation. Audit evidence of the various stages of the CRP development suggested that the identification and assessment of risks, while occurring, was done informally without any documentation of the processes, deliberations or assessment criteria. Further, the audit found the integration of the CRP mitigation responses into the specific detailed directorate workplans to be unclear, creating the potential for misaligned resources. There was also no evidence that the Departmental Management Committee (DMC) was made aware of, or approved of, modifications to CRP mitigation plans.

At a branch and directorate level, several program areas were making good progress in implementing specific risk management tools. While guidance on these tools, including their inter-dependencies and integration processes, are not yet in place, they are a positive step in further integrating risk management into operations and will provide consistent and systematic outputs in the future to inform decision-making processes.

Another key tool at the branch and directorate level that supports operational risks was the Branch Risk Profile (BRP). BRPs are intended to inform each Branch's decision on plans, priorities and resource allocation by capturing, assessing and summarizing key risks that could most impact the achievement of branch objectives. However, the audit found that BRPs were generally not completed or consistently maintained. These operational risks were identified more intuitively rather than systematically or through stakeholder engagement and committee discussions but were generally not documented.

Progress has been made by the DMC to integrate risk information into decision-making activities. Some gaps remain in terms of risk oversight and integration. The audit found senior management generally supportive of risk management, however senior management did not always benefit from a collective discussion and understanding of the Department`s risk tolerances as the risk discussions that did occur at DMC were limited.

At the branch and directorate level the use of risk was more intuitive. Risk management was less structured, largely undocumented, and often only formalized for the purposes of contributing to the required high-level CRP process.

The Departmental Audit Committee (DAC) indicated the importance of not losing track of risks when moving on to the next issue; and the need to use risk information more strategically for such activities as linking resources to the areas of risk and priority.

Audit Opinion

In my opinion the Department's approach to IRM at the strategic level was generally adequate and effective to ensure a consistent approach was used and that risk information was appropriately integrated into decision making. Opportunity exists to further strengthen the approach of IRM at branch and directorate levels to ensure the appropriate integration of risk into decision-making.

Statement of Conformance and Assurance

The audit conforms with the Internal Auditing Standards for the Government of Canada, as supported by the results of the quality assurance and improvement program.

In my professional judgment as Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report. The opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed upon with management. The opinion is applicable only to the entity examined.

Summary of Recommendations

1. Branch Heads should develop annual Branch Risk Profiles or similar tools which ensure risks and opportunities are appropriately identified, assessed, mitigated, and monitored. These Branch Risk Profiles should inform the branch and departmental planning, decision-making, and operational processes.

2. The ADM, Strategic Policy Branch, should develop indicators that inform on the state of implementation of the IRM Policy and Framework.

3. The ADM, Strategic Policy Branch should strengthen the processes surrounding the development, modification, and alignment of CRP mitigation plans into the departmental and branch planning and reporting cycles.

4. The ADM, Strategic Policy Branch, as Chief Risk Officer (CRO) should ensure that DMC has the opportunity to conduct a fulsome review of the departmental strategic risks at minimum twice per year. The CRO should also facilitate the inclusion of appropriate risk information, including those risks identified in the Corporate Risk Profile and the Branch Risk Profiles, into key DMC decision-making activities.

Management Response

The ADM Strategic Policy Branch accepts the results of the audit and commits to pursuing several actions to further support IRM in the Department. The Strategic Policy Branch will also support branches in the implementation of the recommendations that fall under their responsibility as per the departmental IRM Framework and Policy. As well, to the extent possible, the Strategic Policy Branch will support branches in the management of their own risk

processes by providing tools and support, for example through the Community of Practice on Risk.

CAE Signature

_____

Audit Team Members

Deborah Duhn
Melissa Greenland

Acknowledgements

Internal Audit would like to thank the all those who provided advice and assistance during the audit.

1. INTRODUCTION

1.1 Background

As part of the annual risks-based audit planning process, the Department identified integrated risk management (IRM) as an area that should be audited in 2013. The rationale for this decision was also supported as IRM was identified as one of the Department's management priorities in 2013. PS has never audited IRM.

Risk management makes a significant contribution in strengthening capacity to recognize, understand, accommodate and capitalize on new challenges and opportunities. It prepares an organization to respond to change and uncertainty and enables more effective decision-making.

Failure to effectively manage risks can result in increased costs and missed opportunities, which can compromise outcomes, and ultimately public trust. Sound risk management is fundamental to effective public administration as it can lead to a more effective, results-based, and high performance organization.

Risks can include:

- **Strategic risks:** Loss or damage caused by external or systemic conditions or events which may negatively and strategically affect the ability of the Department to achieve its objectives.
- **Operational risks**: Loss or damage caused by people, processes or technology.
- **Hazards:** Loss or damage caused by natural, accidental or pre-meditated actions.

IRM is characterized by several key dimensions:

Dimensions	Description
Horizontal Integration	This refers to the harmonization and alignment of risk management practices horizontally across departmental Branches and programs. Horizontal integration is needed to ensure that consistent approaches for similar risk-based decisions are used, so that overlap and duplication is avoided and that best practices can be shared and leveraged. It is also critical to ensure the appropriate sharing of risk information across the organization, which ultimately enables more informed and robust decision-making.
Vertical Integration	Vertical integration exists when risk management practices at various levels in the hierarchy of the Department are aligned and integrated with one another such that risk information generated at lower levels of the organization can, as appropriate, be consistently aggregated and escalated up to senior management. Vertical integration is needed to ensure that risk information is appropriately shared with senior decision-makers in a way that balances their need to know about, and act on, certain types of risk with lower levels of management's authority to manage.
Functional	Functional integration exists when risk management practices are

Integration	incorporated and integrated directly into existing business functions and decision-making processes. It is vital to ensuring that decisions and managerial functions are, where applicable, appropriately risk-informed and that consistent, efficient and regularized processes exist to ensure that these risk-informed processes are robust and reliable.

International standards[2] and government-wide expectations of good governance emphasize that all types of risks should be considered and integrated into all planning and delivery activities, at the strategic and operational levels. The Treasury Board (TB) *Framework on the Management of Risk* provides guidance to Deputy Heads on the implementation of effective risk management practices at all levels of their organization. This supports strategic priority setting and resource allocation, informed decisions with respect to risk tolerance, and improved results.

The *Management Accountability Framework* (MAF), which is a key performance management tool for the Federal Government, also expects departments to incorporate risk management practices and principles into the organization's strategic, operational and functional activities.

In 2010 Public Safety Canada (PS) approved an *Integrated Risk Management Policy* (IRM Policy) and in 2013, subsequent to the audit period, updated and formally approved the *Integrated Risk Management Framework* (IRM Framework). "This Framework is designed to communicate PS's risk management strategy to all levels of staff, and supply the means to build and maintain a strong risk management capacity. Moreover, it establishes the importance of integrating risk management into the Department's policy, planning, resource allocation and decision-making processes, and creates a link with the organization's strategic documents."[3] The Framework also outlines the key activities in the risk management lifecycle including risk identification, assessment, response, and monitoring.

One of the processes identified within the IRM Framework is the Corporate Risk Profile (CRP) which presents a departmental perspective of the top risks and opportunities by Program at the Program Alignment Architecture (PAA) level. Developed in accordance with the departmental Performance Measurement Framework (PMF), this document, which is now in its third year of implementation, creates a direct link between identified risks and opportunities and expected results identified in the PMF.

Public Safety Canada's Objectives related to Integrated Risk Management[4]

The Department's objectives as they relate to Integrated Risk Management are stated in the Department's IRM Policy and are summarized as follows:

- Implement a process for risk identification and assessment that is comprehensive and systematic;
- Create a management environment that effectively controls and manages risks and allows for appropriate risk-taking within defined parameters;

[2] ISO 31000 Risk Management Principles and Guidelines.
[3] PS *Integrated Risk Management Framework*
[4] PS *Integrated Risk Management Policy*

- Integrate risk management within PS's ongoing activities and management functions, with an emphasis on risk management across Branches and program activities;
- Foster a culture of continuous improvement in risk management through education, training, monitoring and evaluation;
- Promote clear communication and awareness of risk; and,
- Fulfill the requirements outlined in the TB *Framework for the Management of Risk.*

Public Safety Canada's Roles and Responsibilities related to Integrated Risk Management[5]

The ADM, Strategic Policy Branch as the Chief Risk Office (CRO) is responsible for:
- Positioning risk management as an integral component of the Department`s ongoing activities and management functions;
- Determining departmental risk tolerance in consultation with relevant stakeholders;
- Establishing risk management objectives and strategies that align with PS priorities and objectives;
- Developing and monitoring the implementation of risk management guidelines;
- Informing and supporting the Deputy Minister and Management Committee on all identifiable and relevant departmental risks; and,
- Facilitating the opportunity for training on risk management.

The Departmental Management Committee (DMC) is responsible to:
- Promoting the importance of implementing Integrated Risk Management within the Department;
- Determining the most effective way to implement Integrated Risk Management within the Department;
- Incorporating risk management into decision-making;
- Ensuring that corporate risks are properly identified, assessed, managed and discussed at least twice a year;
- Ensuring the capacity to report on the performance of the Department's risk management function; and,
- Ensuring the existence of a supportive learning environment and appropriate communications related to the management of risk.

The Assistant Deputy Ministers are responsible for:
- Integrating risk management into branch management practices;
- Ensuring that branch risks are properly identified, assessed and managed; ensuring that strategic risks are clearly identified through the departmental planning framework and that they are continuously being brought forward to the relevant committees and/or the Deputy Minister, as deemed appropriate;
- Providing clear direction with regard to the appropriate level of response to various types of risk; promoting a supportive environment in which effective risk management and sensible risk taking are encouraged; and,
- Managing levels of risk associated with branch programs, plans and policies.

[5] PS *Integrated Risk Management Policy*

All employees are responsible for:

- Assisting managers with the identification and assessment of risk and developing efficient measures to manage these risks;
- Being proactive about identifying and acting upon risks; and,
- Incorporating risk management as an integral part of business decision-making.

1.2 Audit Objective

The objective of this audit was to provide reasonable assurance that the Department's approach to IRM was adequate and effective to ensure a consistent approach was used and that risk information was appropriately integrated into decision making.

1.3 Scope and Approach

The audit covered the period of September 1, 2011 to December 31, 2012 as this period ensured that findings were current and a complete business management cycle was included. Some of the testing was done on an "under development" basis, examining the processes as they were evolving to provide management with timely advice and insight.

The scope of the audit included all PS Branches and focused on their integrated risk management processes.

The audit reviewed the appropriateness of the Department's fundamental risk management processes, their horizontal and vertical integration into department's decision making processes, and their regular monitoring assuring their ongoing effectiveness.

The audit's focus was on the activities the Department undertook to identify risks within its operational and management activities, however it did not include an examination of the appropriateness or applicability of the individual risk management tools, given their complexity and required subject matter expertise.

1.4 Risk Analysis

PS exerts its leadership and oversight role against the backdrop of internal and external business conditions that expose the Department to a range of operational and strategic risks. Specifically:

- The management of risk in the context of PS is inherently complex. The multitude of players (both within and beyond the Department) that create and use risk information, coupled with varying conceptions of risk and risk tolerance makes the horizontal and vertical sharing of risk information more challenging. Of note is the increasing inter-connectedness of Public Safety programs and priorities, as well as the increasing horizontality of files and issues across government. This inherent horizontality not only increases the need for horizontal sharing of risk information but at the same time, makes it more challenging due to factors such as organizational barriers (silos) and different approaches to risk management throughout the Department and the Government. This is further compounded by an

organizational culture and practice that is more naturally prone to the safeguarding, not disclosure or sharing of risk information, simply because of the business of the Department.

- The nature of PS's mandate is such that managers intuitively manage risk every day, in the course of their operations. This, coupled with the relative newness of formalized risk assessment and risk management practices, makes it more challenging to implement and regularize risk management processes. Efforts to deploy risk management have been positive; however, as with all change management initiatives (particularly during times of resource constraint), there is a risk that IRM may be seen as a mere compliance requirement, rather than a value added function, and that managers revert to past behaviors.

- The impact of resource constraints and the Deficit Reduction Action Plan must also be borne in mind. Reduced resources make it more challenging to invest in new processes; however, risk-based decision-making is an integral tool to assist managers in making tough policy, programming, and resource use decisions.

The detailed risks to which the Department is exposed as a result of this part of its business are summarized in Appendix B. These risks were identified during the planning phase of the audit and were based on extensive interviews and documentation review. The goal of risk-based auditing is to focus the audit examination on the areas that are characterized by the greatest degree of inherent risk. In this way, resources are used efficiently and value to management is optimized. Guided by these risks, the audit's audit objectives, scope and lines of enquiry were identified.

1.5 Audit Opinion

In my opinion the Department's approach to IRM at the strategic level was generally adequate and effective to ensure a consistent approach was used and that risk information was appropriately integrated into decision making. Opportunity exists to further strengthen the approach of IRM at branch and directorate levels to ensure the appropriate integration of risk into decision-making.

1.6 Statement of Conformance and Assurance

The audit conforms with the Internal Auditing Standards for the Government of Canada, as supported by the results of the quality assurance and improvement program.

In my professional judgment as Chief Audit Executive, sufficient and appropriate audit procedures have been conducted and evidence gathered to support the accuracy of the opinion provided and contained in this report. The opinion is based on a comparison of the conditions, as they existed at the time, against pre-established audit criteria that were agreed upon with management. The opinion is applicable only to the entity examined.

2. FINDINGS, RECOMMENDATIONS AND MANAGEMENT RESPONSES

2.1 Policies and Directives

The audit expected to find a clear and appropriately communicated policy, directives, and/or guidelines relating to IRM. It was also expected that employees understand the following:

- the objectives of the Policy;
- their roles, responsibilities and accountabilities;
- how often risks and opportunities should be identified and assessed;
- how risks should be integrated into business-planning, decision-making and operational processes; and,
- how compliance to the Policy is monitored to ensure a continuous learning cycle.

The audit found a well-defined and appropriately communicated PS *Integrated Risk Management Policy* (IRM Policy), and subsequent to the audit examination period, a PS *Integrated Risk Management Framework* (IRM Framework) was approved by senior management. Both documents had identifiable objectives, clear roles and responsibilities, and reporting timeframes which were aligned with the TB *Framework for the Management of Risk* and TB *Guide to Integrated Risk Management.*

The IRM Framework that existed at the time of the audit for all intents and purposes was similar to the recently approved version. It provides guidance on the key activities of a complete risk management lifecycle. A separate quick guide provides a summary of similar risk management notions and approaches, however the audit found that the distribution of the quick guide was limited to the Branch Heads and the participants of the CRP integration sessions as discussed in Section 2.2.1 *Strategic Risk Management Tools*. The audit also found that the guidance concentrated on how risks and opportunities should be identified, assessed and to some extent integrated into planning instruments, however, neither one offered guidance on how to integrate risk management into decision-making or work processes. While the existing guidelines are a good foundation, the TB *Guide to Integrated Risk Management*, articulates a risk-informed approach as "building risk management into existing governance and organizational structures, including business planning, decision-making and operational processes."[6]

The IRM Policy outlines the following processes to monitor the implementation of the Policy:

- Departmental compliance with this Policy may be assessed by Internal Audit, as part of its approved risk-based audit plan. Results of the internal audits will be reported to the Deputy Minister and the Departmental Audit Committee.
- Select monitoring and reviews may also be requested by the Chief Risk Officer to assess changes required to policies, directives, procedures, guidelines and profiles in order to effectively manage risks; and/or to provide reports to the Deputy Minister, as required.[7]

The previous and current version of the IRM Framework stipulates that in order to ensure that integrated risk management is implemented throughout the Department, the following three key mechanisms will be used:

[6] TB *Guide to Integrated Risk Management*
[7] PS *Integrated Risk Management Policy*

- The Strategic Planning Division will promote the application of the IRM Policy in decision-making and planning through the development of tools and mechanisms to facilitate the use of risk information in the Department;
- The TBS Management Accountability Framework (MAF) assessment will highlight best practices and areas of improvement; and
- The Departmental Audit Committee's recommendations will be used by the Strategic Planning Division to improve IRM processes and ensure they are responsive to departmental realities.[8]

While these monitoring mechanisms are positive and will provide some evidence of effectiveness, they remain periodic and at a high-level. There was limited documentation or evidence to support the select monitoring and review of the implementation of the policy. There are no mechanisms that enable timely information on the state of implementation. The audit recognizes that the Strategic Policy Branch (SPB) has succeeded in putting in place many foundational elements with very few resources however a few select indicators would ensure that the momentum gained is not lost. An example of a possible indicator could be the tracking of the completion of Branch Risk Profiles (BRP) which are discussed in section 2.2.3 - Operational Risk Management Tools.

2.2 Risk Management Tools

The audit expected to find tools that would facilitate the full risk management lifecycle. This would include tools that support the management of:

- strategic level risks and opportunities;
- individual specific risk applications, such as the management of grants and contributions; and,
- operational level risks and opportunities.

2.2.1 Strategic Risk Management Tools:

The Corporate Risk Profile (CRP) is the departmental tool which captures the high-level strategic risks. PS has received strong MAF ratings for its CRP process. Additionally, there is positive evidence of the use of the CRP outputs in support of senior management decision-making which will be discussed in Section 2.4 *Integration – Risk Informed Decision-making and Culture*.

On an annual basis each Branch is required to identify their risks and opportunities and bring this information forward for discussion and prioritization at horizontal departmental integration sessions. Each of the identified risks and opportunities were then assessed on the likelihood of occurrence and their impacts. The purpose of these integration sessions is to allow a "challenge" function and more importantly, to ensure that the cross-cutting impacts of these risks and opportunities were appropriately identified and understood departmentally. Following these sessions the top three risks and opportunities by Program level of the Program Alignment

[8] PS *Integrated Risk Management Framework*

Architecture (PAA) formed the CRP. Responsible Directorates and mitigation plans were then identified for each strategic risk or opportunity.

Identifying Strategic Risks:

Generally all interviewees indicated that branch meetings were held to identify potential risks related to their areas of responsibility in preparation for the CRP integration sessions. They also indicated that these risks were informed by other inputs such as outputs from their specific use risk management tools, which are presented in section 2.2.2, stakeholder consultations, and inter-departmental committees. The audit found that the approaches to inform and assess the risks were not documented. Consequently, it was not possible to determine the completeness and sufficiency of this risk identification step and whether some operational and strategic risks were overlooked. The absence of documentation may also contribute to a misunderstanding and/or misinterpretation of the basis of these risks.

The audit noted that in some cases the input of risks for certain PAA level Programs was limited in quantity; for example one Program identified only four high-level risks. Given the complexity and sensitivity of each Program, the audit expected more detailed lists. The audit did not attempt to assess the sufficiency, validity, and relevancy of these risks. The limited number did raise concerns as to whether the Department has overlooked any risks and whether the process benefited from a robust horizontal "assessment and challenge".

Assessing Strategic Risks:

Interviewees indicated that the integration sessions were important in providing an opportunity for all participants to understand the departmental risk environment as well as the proposed mitigation plans and acceptable tolerances. Although there was no evidence to support the deliberation of these sessions, it was noted by participants that their ability to report back to their colleagues on a department-wide risk perspective contributed to a heightened risk awareness and knowledge.

The CRP presents the top three risks and opportunities for each Program level of the PAA. As a result it is possible that risks ranking lower than the top three within one specific Program, but higher than the top three risks of other Programs will not be included in the CRP. Consequently, there is no mechanism in place that ensures that the Department's highest ranking strategic risks are managed corporately and monitored by the most senior governance committees.

Developing Risk Responses for Strategic Risks:

CRP risks and mitigation plans are developed in the fall as part of the regular departmental planning and reporting cycle. This information is then prepopulated by the Strategic Policy Branch into the Branch Business Plans (BBP) to ensure continuity. It is then expected that branches appropriately update the mitigation plans into the respective directorate workplans. This exercise is positive in that it ensures that all CRP risks and mitigation plans are assigned to the appropriate branches.

To better understand the alignment of the risks and the associated mitigation plans, the auditors developed a cross-walk between the risks identified in the CRP to the risks identified in the business plans to the actions identified in the directorate work plans. The audit was able to trace the CRP outputs into the BBPs.

As expected, the directorate workplans contained detailed actions that were intended to address the high level CRP mitigation plans. However it was not always clear whether:

- the mitigation plans identified responded to the original high level CRP mitigation plans,
- the mitigation plans cascaded into the individual directorate workplans as appropriate, and,
- changes to the mitigation plans were reassessed to ensure they still sufficiently mitigated the risks.

There was also no evidence that DMC was made aware of, or approved, modifications to CRP mitigation plans.

An example that highlighted the potential misalignment between the CRP mitigation plans and the directorate workplans was observed in one of the 2011-12 CRP risk statements: "That the Government Operations Centre (GOC) infrastructure may not support a coordinated response to an event affecting the national interest – space, security, survivability, and sustainability requirements." This risk statement and the related mitigation plans remained unchanged through to 2013-14. It was uncertain whether the CRP mitigation plans and the associated directorate workplans were either not addressed or not sufficient, or whether the Department chose to accept the risk without mitigating it.

2.2.2 Specific Use Risk Tools:

As part of the audit the following program areas specific use risk management tools were examined:

- *Public Safety Information Management System* (PSIMS) which captures risk information for individual recipients for departmental grants and contribution programs;

- *All Hazards Risk Assessment tool* (AHRA) which, led by PS, in close partnership with Defense Research Development Canada - Centre for Security Science, supports all federal government institutions in fulfilling their legislative responsibility to conduct mandate-specific risk assessments as the basis for Emergency Management planning; and,

- *Critical Infrastructure tool* which was developed to support the goal of the National Strategy for Critical Infrastructure in partnership with federal, provincial and territorial governments and critical infrastructure sectors for the purpose of improving information sharing and protection and sustaining a commitment to all-hazards risk management. This all-hazards approach considers: natural hazards; accidental hazards, and intentional threats.

The audit found the development of these specific use risk management tools to be a very positive step in fulfilling risk management and providing outputs to inform decision-making processes in support of these program areas.

It was indicated that these tools were in the early stages of implementation and therefore did not yet provide consistent and systematic outputs. The audit also noted that there was limited documented guidance to support how these tools were to be integrated into other risk-informed operations such as:

- how inter-dependencies and information should be shared;
- how outputs should be integrated into directorate, branch and departmental risk management activities; and,
- how these tools should support the complete risk management lifecycle including response and monitoring.

While the tools supported risk identification, assessment, and some aspects of response, none of the tools had defined approval, reporting and monitoring mechanisms or processes.

2.2.3 Operational Risk Management Tools:

Branch Risk Profiles (BRP) as identified in the PS *Integrated Risk Management Framework* are intended to inform each Branch's decision on plans, priorities and resource allocation by capturing, assessing and summarizing key risks that could most impact the achievement of branch objectives. Once finalized the BRPs are used to drive discussions in the development of the CRP.

The audit found that BRPs were generally not completed or consistently maintained nor did branches have any other consolidated risk document. In the instances where branches had a documented BRP, its content was essentially the same as the CRP risks with little additional information. Employees did not use any specific use or operational risk management tools to identify, assess, respond and monitor risks associated to policy development or research activities. Rather the audit was told that these risks were identified through undocumented intuitive means or through stakeholder engagement and committees.

Without having a consolidated risk document, risk management is fragmented and disconnected and consequently the department cannot easily be assured of the completeness and consistent interpretation of risk information and that all risks are appropriately considered throughout the planning and reporting stages. This may also impact the integrity of the planning process and may jeopardize the achievement of better performance.

2.3 Governance

The audit expected to find governance structures that promote a risk informed culture and management practices throughout the Department. It was also expected that departmental governance structures would monitor the management of risks, and the implementation of the IRM Policy and Framework. The audit examined the following departmental committees:

- Departmental Management Committee;
- Departmental Audit Committee; and,

- Branch and Directorate Management Committees.

Departmental Management Committee (DMC):

The DMC terms of reference states that the committee`s objectives are to review and approve policies, projects, plans, performance, and reports relating to a broad and diverse suite of corporate management programs and services for the Department including risk management. Further the IRM Policy requires that the DMC identify, assess, manage, and discuss corporate risks at least twice per year.

The audit found:

- In 2012-13 DMC did not review the initial CRP update as it was approved bi-laterally with the DM. The audit was informed that there were opportunities for all members to review and provide their input individually. However, members did not benefit from a collective discussion allowing for the understanding of the Department`s risk tolerances.

- An update on the risks and their respective mitigation plans was presented during the mid-year review process. Interviewees noted that there was limited discussion, only twenty minutes were allotted on the agenda for the entire mid-year review of performance and risk; this is not conducive to a fulsome discussion. Further the documentation supporting the mid-year discussion only included a "symbol" indicating risk status. The onus was on each individual ADM to determine what to present. The audit expected a more deliberate discussion and consistent presentation of strategic risks and their mitigation by the senior management team.

- Finally the audit noted that the onus was on individual presenters to the DMC to determine the criteria for the disclosure of risk information.

The Departmental Audit Committee (DAC):

DAC, which provides advice on such areas as risk management, was informed of "risks" and risk management processes on a regular basis throughout the audit period. DAC commended the progress made in the implementation of IRM. It was noted that this committee actively uses the outputs from the CRP to challenge departmental activities such as resource allocations. Advice from the Committee members focused on the importance of not losing track of risks when moving on to the next issue; and the need to use risk information more strategically for such activities as linking resources to the areas of risk and priority.

Branch and Directorate Management Committees:

Branch and Directorate management committees were identified as fundamental governance structures. However none of these meetings had specific terms of reference or other agreed upon processes defining "when" or "what" risk information should be presented. Nor were any of the meeting discussions documented, thereby making it challenging for audit to conclude whether these committees were providing any form of risk oversight. Compounded by the absence of

BRPs as presented in section 2.2.3 – Operational Risk Management Tools, and the lack of directorate risk information within the BBP, the audit could not conclude whether risk information was being used to inform decision-making.

Without defined information requirements, documented discussions, and rigor in ensuring compliance, sufficient and appropriate risk information including risk tolerances and mitigation status, risks may not be effectively reported and monitored. Organizations may be keeping information that prevents them for achieving objectives and the highest of performance.

2.4 Integration – Risk Informed Decision-making and Culture

The audit expected to find risk-informed approaches to business planning, decision-making, and operational processes. As stated in the PS *IRM Framework*, "the objective is to create an environment where all levels of the organization will instinctively look for risk and opportunities and take into account their impacts on departmental outcomes when making decisions at both the operational and the corporate levels."[9]

Departmental Level:

The audit found that senior managers have started to integrate risk information into key decision-making activities as "risk" has become more engrained. The inclusion of risk information has largely been done through the use of the CRP outputs and specific risk information presented to DMC. The audit noted the following examples:

- The Banking Day exercise which re-allocates resources to new funding pressures now prioritizes the status of implementation of the CRP risk mitigation plans before considering other pressures.

- The *Risk and Results Based Approach to Staffing* developed by the Human Resources Directorate, informs delegated managers on the risk tolerances of senior management for different types of staffing actions and categorizes them such that controls and reporting requirements are commensurate to the different levels of risks.

- During the development of the departmental priorities, SPB incorporated the CRP outputs into the planning process ensuring the visibility of risks and opportunities and their alignment to each priority. The CRP outputs were further used in the development of the *Report on Plans and Priorities*. The integration of risks in this manner was a positive step in guiding the focus of the Department.

Even so, there continues to be gaps in regard to integrating risk information in decision-making. For example, there was no systematic requirement for risk management information to be included in briefing notes, memos, status reports, or financial and non-financial performance reports.

[9] PS *Integrated Risk Management Framework*

The audit did note, the Strategic Planning Division, Strategic Policy Branch has started a *Risk and Threat Assessment Community of Practice,* which will provide a valuable means of tapping into departmental strengths, and to share tools, information, and expertise both horizontally and vertically on an ongoing basis. This forum will provide an opportunity to learn and collaborate where possible and possibly reduce duplication of efforts.

Departmentally the audit found senior management generally supportive of risk management and that tolerances for certain risks were communicated to lower levels. Examples of the mechanisms used to establish a risk management environment included the official approval and communication of the IRM Policy, and the completion and communication of the annual CRP.

However, as noted in previous audits a culture of silos still persists in some areas which impede broad and transparent departmental risk discussions. Without building the transparency and trust needed for a comprehensive risk understanding, departmental risks strategies and tolerances may not be clearly communicated leading, to sub-optimal decisions and use of resources.

Branch/Directorate level:

As noted earlier there were generally no BRPs and few operational risk management tools to facilitate risk awareness and understanding. Generally, at the Branch and Directorate level the use of risk was more intuitive. Risk management was less structured and often only formalized for the purposes of contributing to the required high-level CRP process or applied for a specific program need such as the management of contribution recipients. A number of interviewees noted that the CRP outputs were of limited use and perceived it to be an administrative task with minimal value-add. Therefore in some cases it did not guide their decision-making activities.

Generally interviewees noted that information related to finances, HR capacity, and stakeholder concerns were the key sources that informed decision-making. Risks per say were not the focus of discussions. These indicators in and of themselves are not sufficient to enable robust integrated risk management.

While there were positive signals that some decisions were informed by risk, without a more structured and deliberate risk-informed approach, there is a risk that sub-optimal decisions may be made.

Recommendations

1. Branch Heads should develop annual Branch Risk Profiles or similar tools which ensure risks and opportunities are appropriately identified, assessed, mitigated, and monitored. These Branch Risk Profiles should inform the branch and departmental planning, decision-making, and operational processes.

2. The ADM, Strategic Policy Branch, should develop indicators that inform on the state of implementation of the IRM Policy and Framework.

3. The ADM, Strategic Policy Branch should strengthen the processes surrounding the development, modification, and alignment of CRP mitigation plans into the departmental and branch planning and reporting cycles.

4. The ADM, Strategic Policy Branch, as Chief Risk Officer (CRO) should ensure that DMC has the opportunity to conduct a fulsome review of the departmental strategic risks at minimum twice per year. The CRO should also facilitate the inclusion of appropriate risk information, including those risks identified in the Corporate Risk Profile and the Branch Risk Profiles, into key DMC decision-making activities.

#	Management Action Plan	Planned Completion Date
1	The Emergency Management and Regional Operations Branch will participate in a risk management pilot. All Branch Heads will develop an annual Branch Risk Profile or similar tool to ensure risks and opportunities are properly assessed, mitigated and monitored.	January 31, 2014 October 31, 2013
2	Strategic Planning Division will continue to participate in the annual MAF exercises which provide an assessment of the implementation of IRM in the Department. Strategic Planning Division will identify a set of indicators that will inform on the state of implementation. The status of these indicators will be reported on in the annual Corporate Risk Profile document.	January 31, 2014
3	Strategic Planning Division will review the business planning process to ensure that mitigation strategies can be easily transferred and clearly represented in all business plans. In addition, the Strategic Planning Division will play a greater challenge function during integration session to ensure the inclusion of mitigation strategies. As part of the 2014-15 business planning process, Strategic Planning Division will also assist Branches with the integration of mitigation strategies into their plans. Strategic Planning Division will also be implementing a pilot project to enhance risk-based management at the Branch-level.	April 30, 2014
4	Each ADM will be provided with a copy of the most recent CRP at each key decision-making DMC meeting such as priority-setting, banking day, and mid- and end-of-year reviews. The CRP will be used to guide the discussions and decisions. During the development of the CRP, the ADM, Strategic Policy Branch, will provide DMC with a status update at each phase. At the	October 31, 2013 January 31, 2014

	identification phase, DMC will be provided with a draft list of the proposed top risks and opportunities; at the assessment phase, DMC will be provided with a draft list of proposed risk scores; and at the response stage, DMC will be provided with a draft of the proposed mitigation strategies. DMC will have the opportunity to provide comments throughout the development in addition to on the final draft.	

ANNEX A: AUDIT CRITERIA

Lines of Inquiry
Line of Inquiry 1: Policy and Direction The Department has a formally defined, communicated and adequate policy and direction in relation to risk management.
Line of Inquiry 2: Governance The Department has adequate and effective governance over Integrated Risk Management which would include clear roles, responsibilities and accountabilities, and oversight mechanism. Note: This includes such things as: - Tone at the top - Accountabilities of SPB and other Branches - Oversight by DMC, Monitoring - Champion - Approval authority over risk reports, including escalation
Line of Inquiry 3: Business Processes and Tools Comprehensive risk management tools and processes exist, are communicated and are applied in conformity with departmental policy and direction. Risk Management Tools include methods for all aspects of the risk management lifecycle including: - Risk identification - Risk assessment - Response – action planning (based on tolerance) - Approval – of all aspects of the risk assessment, response etc. - Communication/Escalation
Line of Inquiry 4: Integration and Use of Risk for Decision Making Risk information is systematically used to inform key decisions, in conformity with the departmental directions and requirements on risk management. Including vertical and horizontal information sharing.

ANNEX B: PRELIMINARY AUDIT RISKS

As a result of these conditions and the risk factors that stem from them, the following is a summary of the key risks to which PS is exposed in relation to Integrated Risk Management.

Risk Name	Description
1. **Culture**	There is a risk that organizational culture and operating practices will not allow for or compel the optimal sharing of information and discussion of risk information.
2. **Business Process – Application of Tools**	There is risk that risk management tools will not be applied consistently or in an appropriately robust fashion.
3. **Inputs**	There is risk that individual risk management processes will not be informed by comprehensive inputs.
4. **Vertical Integration**	There is a risk that the corporate risk profile and decisions resulting from it will not be appropriately informed by existing lower level risk management processes and resulting risk information.
5. **Horizontal integration**	There is risk that there will be insufficient sharing of risk information across Branches and Directorates.
6. **Functional Integration:**	There is a risk that managerial functions and decisions (e.g., priorities, resource allocation/re-allocation, program decisions) will not be properly informed by risk information.
7. **Response & Monitoring**	There is a risk that risks will not be formally and appropriately responded to and monitored