Innovation, Science and Economic Development Canada

Innovation, Sciences et Développement économique Canada

AUDIT OF INTEGRATED RISK MANAGEMENT
FINAL REPORT

AUDIT AND EVALUATION BRANCH
OCTOBER 2018

Canada

This publication is available online at https://www.ic.gc.ca/eic/site/ae-ve.nsf/eng/h_00350.html

To obtain a copy of this publication or an alternate format (Braille, large print, etc.), please fill out the Publication Request Form at www.ic.gc.ca/Publication-Request or contact:

Web Services Centre
Innovation, Science and Economic
Development Canada
C.D. Howe Building
235 Queen Street
Ottawa, ON K1A 0H5
Canada

Telephone (toll-free in Canada): 1-800-328-6189
Telephone (Ottawa): 613-954-5031
TTY (for hearing-impaired): 1-866-694-8389
Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)
Email: info@ic.gc.ca

Cat. No. Iu4-235/2019E-PDF
ISBN 978-0-660-28920-5

Aussi offert en français sous le titre *Audit de la Gestion Intégréé des Risques*

TABLE OF CONTENTS

LIST OF ACRONYMS USED IN REPORT

ADM	Assistant Deputy Minister
AEB	Audit and Evaluation Branch
CAE	Chief Audit Executive
CFO	Chief Financial Officer
CIPO	Canadian Intellectual Property Office
CMS	Corporate Management Sector
DAC	Departmental Audit Committee
DGMAC	Director General Management Advisory Committee
DMC	Departmental Management Committee
DPPM	Departmental Project and Program Management
IPR	Integrated Planning and Reporting
IRM	Integrated Risk Management
ISED	Innovation, Science and Economic Development
ISO	International Standardization Organization
NODP	Northern Ontario Development Program
STS	Spectrum and Telecommunications Sector

1.0 EXECUTIVE SUMMARY

1.1 INTRODUCTION

The primary goal of every organization is to deliver on its objectives, and risk is the uncertainty an organization faces in trying to meet those objectives. An organization may be faced with internal risks, which arise from the normal operations of a business, and external risks, which arise from the broader business environment. Risk management involves making informed decisions on which risks to manage, rather than attempting to manage all risks. Further, it should be integrated into the organization's governance, structures, and programs to ensure that risks are not managed in isolation.

The Treasury Board *Framework for the Management of Risk* outlines a principles-based approach to risk management for departments and agencies. Effective risk management, supported by this framework, enables departments to identify and manage different types of risks at all levels of their organization, provide guidance on setting risk tolerance levels, and make informed decisions.

At Innovation, Science and Economic Development (ISED), the risk management process is performed as part of a broader departmental Integrated Planning and Reporting (IPR) process, led by the Corporate Management Sector (CMS). The IPR process is a coordinated department-wide exercise designed to identify key priorities, risks and opportunities, and supports the development of the Department's Corporate Plan, which includes the Corporate Risk Profile.

1.2 AUDIT BACKGROUND

The objective of the audit was to provide assurance that ISED has an Integrated Risk Management (IRM) Framework that is being used consistently to identify and assess risks for planning, oversight, and decision-making purposes.

The audit scope focused on ISED's Integrated Risk Management (IRM) Framework as it relates to risk management activities undertaken at the corporate, sector and operational level, from April 1, 2016 to September 30, 2017 including:

- Roles and responsibilities;
- Governance processes;
- Communication mechanisms;
- Risk management processes;
- Risk management tools; and
- Activities related to risk management awareness and innovation efforts.

1.3 OVERVIEW OF AUDIT RESULTS

Strengths

ISED's Corporate Governance Framework defines the Department's Integrated Planning and Reporting (IPR) process, which includes risk management activities. Leveraging the IPR process, a Corporate Risk Profile is developed annually.

Some good practices were noted in sectors, which included a tailored integrated risk management framework, and multiple initiatives to develop more formalized risk management activities and tools. At the program and project levels, processes and tools for risk management are in place, and examples of tools being used in programs were found with consideration of risk tolerance.

Areas for Improvement

Some opportunities for improvement were identified by the audit. Accountabilities, roles and responsibilities related to risk management are not clearly defined and are not commonly understood across sectors. There is no process in place to integrate sector risk information in the Corporate Risk Profile, and there are no standard risk categories or guidance on risk tolerance or risk thresholds for sectors to consider when performing risk assessments.

Risk management activities vary across sectors, with some sectors having developed risk processes and tools, while processes in other sectors are informal.

Finally, there is limited guidance and communication to support risk management activities, including building risk management capacity, and continuous improvement is not embedded in risk management practices.

1.4 AUDIT OPINION AND CONCLUSION

Risk management activities are taking place at the corporate, sector and operational levels. However, the Department would benefit from more attention to risk management, supported by more formal processes, additional documentation, and regular monitoring at the corporate and sector levels. The Department would also benefit from more guidance and communication from the corporate function to support sectors' risk management practices.

1.5 MANAGEMENT RESPONSE

Management has agreed with the findings included in this report and will take action to address all recommendations by March 31, 2020.

1.6 STATEMENT OF CONFORMANCE

This audit was conducted in accordance with the Internal Auditing Standards for the Government of Canada, as supported by the results of the Audit and Evaluation Branch's quality assurance and improvement program.

_____

Michelle Gravelle
Chief Audit Executive
Innovation, Science and Economic Development

2.0 BACKGROUND

2.1 OVERVIEW OF INTEGRATED RISK MANAGEMENT

The primary goal of every organization is to deliver on its objectives, and risk is the uncertainty an organization faces in trying to meet those objectives. All activities involve risks to varying degrees, and risks can involve both threats and opportunities. An organization may be faced with internal risks, which arise from the normal operations of a business, and external risks, which arise from the broader business environment.

Risk management is defined as a set of coordinated activities to direct and control an organization with regard to risk1. It involves setting the best course of action under uncertainty by identifying, assessing, understanding, making decisions on, and communicating risk issues. Risk management does not necessarily mean risk avoidance in the case of threats and it should be viewed as key to good decision-making. Moreover, risk management involves making informed decisions on which risks to manage, rather than attempting to manage all risks.

Risk management enables an organization to:

- Increase the likelihood of achieving its strategic objectives;
- Encourage proactive management of risk;
- Improve the identification of opportunities and threats;
- Comply with relevant legal and regulatory requirements and adhere to international norms;
- Improve operational effectiveness and efficiency;
- Improve governance and internal controls; and
- Establish a reliable basis for informed decision-making, resource allocation, and planning.

Risk management should not be undertaken in isolation but rather, it is expected that organizations develop, implement and continuously improve a risk management framework that integrates risk management into the organization's governance, structures, and programs. The framework provides the overall context for risk management in an organization and supports the understanding and communication of risks from an organization-wide perspective. It includes the instruments needed at all levels of an organization to manage risks, such as policies, accountabilities, resources, activities and reporting mechanisms.

In addition, a risk management framework sets out a risk management process, which provides an organization with a specific set of steps for identifying, assessing, mitigating and monitoring risks in a consistent manner. This process should be periodically reviewed to ensure its continued relevance and effectiveness.

Concretely, the risk management framework and process should be integrated in an organization's business planning cycle through which planning activities set strategic direction, priorities and key milestones for programs and service delivery. As part of these planning

[1] International Organization for Standardization (ISO) International Standard 31000:2009(E).

activities, risks should be identified, assessed and prioritized, and a determination made as to which risks require mitigation. This risk information then informs the development of an organization's operational plans, including investment decisions. Action plans to respond to risks should be developed and risk-based monitoring and reporting embedded into operations and programs.

Good practices in risk management include identifying lessons learned in order to support continuous improvement, with adjustments made as needed. As well, the results of the integrated business planning cycle should be communicated to internal and external stakeholders to support risk awareness, to provide opportunities for feedback (e.g. extent to which risks are adequately identified), and to bring together different areas of expertise to assess risk.

2.2 RISK MANAGEMENT IN THE FEDERAL GOVERNMENT

The Treasury Board *Framework for the Management of Risk* outlines a principles-based approach to risk management for departments and agencies. The framework enables departments to identify and manage different types of risks at all levels of their organization, to provide guidance within their organization on setting risk tolerance levels, and to make informed decisions.

The Framework's key principles require that risk management in the federal government:

- Support government-wide decision-making and priorities, as well as the achievement of organizational objectives and outcomes, while maintaining public confidence;
- Support internal decision-making by enabling organizations to identify and manage risks which are specific to their own objectives and expected outcomes;
- Be tailored and responsive to the organization's external and internal context, including its mandate, priorities, organizational risk culture, risk management capacity, and partner and stakeholder interests;
- Add value as a key component of decision-making, business planning, resource allocation and operational management;
- Be transparent, inclusive, integrated and systematic; and
- Achieve a balance between the level of risk responses and established controls and support for flexibility and innovation to improve performance and outcomes.

2.3 RISK MANAGEMENT AT INNOVATION, SCIENCE AND ECONOMIC DEVELOPMENT

At Innovation, Science and Economic Development (ISED), risk management activities are led by the Corporate Management Sector (CMS), and a departmental framework describes concurrent processes at the corporate level, in sectors, and in functional areas:

- **Corporate level**: Identify, assess and mitigate key risks that could impede ISED's ability to achieve its mandate or priorities. This process is centralized and coordinated by CMS, with sector input.

- **Sectoral level**: Identify, assess, and mitigate risks which could impede sectors' ability to achieve their priorities or program targets based on each sector's business needs. This

process is decentralized, providing flexibility to Sector heads on how to manage their risks according to their business needs.

- **Functional areas**: Functional areas have risk management and risk-based decision-making processes built into their day-to-day operations, namely grants and contributions funding, project management, and security.

Risk management activities are driven by the Integrated Planning and Reporting (IPR) process, led by CMS, as illustrated in Appendix A. The IPR process is a coordinated department-wide exercise designed to identify key priorities, challenges, risks, trends and opportunities. The IPR process supports the development of the Department's Corporate Plan, which includes ISED's Corporate Risk Profile.

3.0 ABOUT THE AUDIT

In accordance with the approved Innovation, Science and Economic Development 2016-17 to 2019-2020 Risk-Based Internal Audit Plan, the Audit and Evaluation Branch (AEB) undertook an audit of integrated risk management.

3.1 AUDIT OBJECTIVE

The objective of the audit was to provide assurance that ISED has an Integrated Risk Management (IRM) Framework that is being used consistently to identify and assess risks for planning, oversight, and decision-making purposes.

3.2 AUDIT SCOPE

The audit scope focused on ISED's Integrated Risk Management (IRM) Framework as it relates to risk management activities undertaken at the corporate, sector, and operational level, from April 1, 2016 to September 30, 2017 including:

- Roles and responsibilities;
- Governance processes;
- Communication mechanisms;
- Risk management processes;
- Risk management tools; and
- Activities related to risk management awareness and innovation efforts.

3.3 METHODOLOGY

The audit was conducted in accordance with the Internal Auditing Standards for the Government of Canada.

Based on the identified risks, AEB developed the audit criteria and sub-criteria linked to the overall audit objective (see Appendix B).

The methodology used for this audit included performing various procedures to address the audit's objective. These included a review of documentation, interviews, walkthroughs, and a review of a sample of ten programs and four projects to assess risk management frameworks, as well as risk processes and tools, in operational environments (see Appendix C).

The sample was selected to ensure appropriate coverage of:

- ISED's Core Responsibilities and Program Inventory as set out in the Departmental Results Framework;
- Programs in the Program Inventory with values over $60M;
- Functional areas;
- Grants and contributions, selected based on materiality; and
- Programs with limited audit exposure.

Sectors were included in this engagement in order to assess their respective risk management frameworks, including processes and tools to identify, monitor, and mitigate risks. Past audit findings were also reviewed to inform how risk management has been assessed in recent years.

A debrief meeting was held with the Chief Financial Officer and Assistant Deputy Minister, CMS, on August 2, 2018, to validate the findings that form the basis of this report. This meeting also provided the auditee an opportunity to offer any additional information and clarification regarding the findings.

4.0 FINDINGS AND RECOMMENDATIONS

4.1 INTRODUCTION

This section presents detailed findings from the audit of Integrated Risk Management. The findings are based on evidence and analysis from both the initial risk assessment and the detailed audit work.

4.2 GOVERNANCE

A number of governance committees are in place at the corporate level at which risks are discussed. However, accountabilities, roles and responsibilities for risk management activities are not clearly defined and are not commonly understood across sectors.

Risk management is integral to strategic and operational planning, as risks represent uncertainty over an organization's ability to deliver on its mandate. A governance framework should ensure that risk management supports priority-setting and decision-making, and is fully integrated into the planning process. As with all governance frameworks, roles and responsibilities related to risk management should be well-defined and clearly understood by all parties to ensure the process unfolds as intended.

ISED has established a governance model designed with the objective of ensuring the Department's activities and decisions are managed coherently and strategically. It is intended to support departmental officials in exercising their collective responsibility to ensure sound and strategic management of the Department's affairs. Under this model, corporate governance structures and processes, including senior departmental committees and the Department's integrated business planning cycle, are the means through which ISED establishes corporate priorities, strategies, policy instruments and processes.

The ISED Corporate Governance Framework defines at a high level the roles and responsibilities for senior officials, including the Chief Financial Officer (CFO), Chief Audit Executive (CAE), and Sector Heads. However, accountabilities, roles, and responsibilities related to risk management are not defined at the corporate or sector level.

The Framework also defines roles and responsibilities for senior governance committees. Oversight committees responsible for risk discussions are:

- Departmental Management Committee (DMC): provides strategic direction and oversight of ISED public policies, programs and services, as well as its management of resources. As the senior decision-making committee in the Department, the committee is

responsible for providing direction on and endorsing proposed strategies, frameworks, plans, and activities, including risk assessment and mitigation.

- Director General Management Advisory Committee (DGMAC): examines proposals affecting the management of the Department and the stewardship of its resources – its people, finances, information, systems, services, and assets – prior to their review by DMC.
- Departmental Audit Committee (DAC): provides objective advice and recommendations to the Deputy Minister on the sufficiency, quality and results of internal audit engagements related to the adequacy and functioning of the Department's risk management, control and governance frameworks and processes.
- Corporate Services Network (CSN): shares information on corporate strategies, plans, issues, initiatives, investments, as well as management priorities and practices to ensure that sectors remain informed about the direction and discussions affecting corporate services in the Department.

Risk discussions were held at these senior governance committees with a focus on identifying corporate risks for ISED's 2017-18 Corporate Plan with consideration given to the recent departmental realignment and the implementation of Canada's Innovation and Skills Plan. Although the risks presented in the Corporate Plan were documented as part of these discussions, the nature and depth of the risk discussions are undocumented.

Governance activities with respect to risk management vary across sectors. Good practices were identified in the Spectrum and Telecommunications Sector (STS) and the Canadian Intellectual Property Office (CIPO), both of which have defined roles and responsibilities, as well as documented decisions related to risk management by their oversight committees.

However, roles and responsibilities related to risk management are not consistently defined and documented across all other sectors, nor are they commonly understood. Many sectors perceive the Corporate Management Sector (CMS) to be the only group responsible for risk management activities, and sectors are not clear on their responsibilities for sector-level risk management and expectations to perform any related activities outside of the IPR process. Senior management meetings were identified in interviews as the main governance vehicle to discuss risks across sectors, but these discussions were not documented and were held on an *ad hoc* basis.

Without clear accountabilities for risk management at the corporate and sector levels, the Department's ability to deliver on its priorities or meet its strategic objectives may be hindered. Further, if roles and responsibilities related to risk management are not defined and commonly understood, risk management activities could be inconsistent, not aligned with organizational objectives, or non-existent.

Recommendation 1 (Medium Risk):

CMS should define and communicate accountabilities, roles, and responsibilities for risk management activities at the corporate and sector level.

4.3 CORPORATE RISK MANAGEMENT PROCESS

A process exists to develop the Corporate Risk Profile as part of the Integrated Planning and Reporting process. However, the information provided by sectors through this process is not being leveraged. Further, there are no standard risk categories or guidance on risk tolerance or risk thresholds for sectors to consider when performing risks assessments.

The Integrated Planning and Reporting (IPR) process is a coordinated department-wide exercise designed to identify key priorities, challenges, risks, trends and opportunities. The IPR process is intended to support the execution of individual and collective accountabilities through reporting on progress, performance and results. Much of the strategic, financial, and operational data that informs the Department's planning and decision-making processes is gathered through this annual exercise. This includes risk management, the results of which are reflected in ISED's Corporate Plan.

As part of the IPR process, sectors provide input to CMS on their key deliverables and sector-specific risks for a given period. The process is managed through a formal call-out from CMS to sectors, which includes templates to be completed by sectors. These templates include general instructions on defining the impact and the likelihood of a given risk. However, they do not include a standard set of risks or risk categories for sectors to consider when performing the risk assessment, nor is there guidance on risk tolerance or on risk thresholds for the Department to ensure consistency in the risk identification process. As a result, the level of risk information submitted to CMS as part of the IPR process varied across sectors.

The sectors' input is intended to inform the identification of corporate risks to be included in the Corporate Risk Profile, as illustrated in Appendix D, and presumes that risk management is being performed at the sector level. The Corporate Risk Profile sets out the key risk areas that could impact the organization in achieving its objectives, along with mitigation plans for the risks identified. In practice, sector input is not analyzed or leveraged by CMS, as ISED's Corporate Risk Profile is currently determined based on a review of the previous year's corporate risks, as well as risks identified by senior management through discussions undertaken at DMC and DGMAC. Once corporate risks are defined, mitigation plans are developed by sectors identified as risk owners and submitted to CMS through the IPR process. However, there is no monitoring of the mitigation activities for corporate risks to determine whether they are being managed effectively.

Not having standard risk categories or guidance on risk tolerance or risk thresholds may result in inconsistent risk identification and risk management across the Department, and could leave key risks ignored. A lack of aggregation and analysis of sector risk information reduces the ability to strategically identify risks that could most impact the Department's capacity to deliver its mandate. Finally, not having a process for monitoring mitigation activities as a response to the identified risks could lead to unmanaged corporate risks.

Recommendation 2 (High Risk):

CMS should develop, communicate, and implement a corporate risk methodology and process which includes standard risk categories, and guidance on departmental risk tolerance and risk thresholds.

Recommendation 3 (High Risk):

CMS should leverage and analyze information provided by sectors to inform the Corporate Risk Profile, as well as define and implement a process for monitoring mitigation activities for corporate risks.

4.4 OPERATIONAL RISK MANAGEMENT PROCESS

Risk management activities vary across sectors, with some sectors having developed risk processes and tools, while processes in other sectors are informal. At the program and project levels, processes and tools for risk management are in place.

Alignment of risk management practices across sectors, programs, and projects, as well as the consistent use of tools, can support an organization in its ability to effectively integrate risks and mitigation strategies both horizontally and vertically. This integrated view encourages a portfolio approach to risk management, and can help to reduce siloed processes and decision-making. A fully integrated framework would also include performance information, with targeted outcomes directly associated with risk assessment and mitigation activities.

Sector Level

The consistency and maturity of risk management activities vary across sectors. Several good practices were identified, including in the Canadian Intellectual Property Office (CIPO), where an integrated risk management framework has been developed and includes specific risk management accountabilities, including compliance and oversight; integration processes for risk management with tools for risk recording; monitoring, reporting and communications processes; a program risk and issue management strategy; and a risk register.

There are additional sectors and branches undertaking risk management improvement initiatives, such as the Competition Bureau and Corporations Canada, which have each developed environmental scan processes to support risk identification; and the Spectrum and Telecommunications Sector, which recently began the development and implementation of a risk management framework.

Risk management practices in the remaining sectors are often informal, and are described as taking place mainly through senior management meetings. Further, there are no sector-level risk frameworks or sector risk profiles beyond those mentioned above, and limited risk management processes and tools in place.

Without sector-level risk frameworks or sector risk profiles, decision-makers may not have a complete and cohesive view of the Department's risk environment. A lack of sector-level processes and tools for identifying, assessing, managing and monitoring risks could reduce an organization's ability to effectively integrate and align risk management activities to the corporate framework.

Program and Project Level

All sampled programs and projects demonstrated the use of processes and tools for the integration of risk management in planning, operations and reporting activities. For the sampled programs, risks were identified in Treasury Board submissions, and related mitigation actions were defined in contribution agreements. For the sampled projects, risks were identified and mitigation strategies were included in the Department Project and Portfolio Management (DPPM) online system tool.

There were also examples of defined understandings of risk tolerance for individual programs including the Canada Small Business Financing Program and Northern Ontario Development Program (NODP), which included defined tolerances and associated mitigation measures. The NODP uses a program-specific tool that assesses risks for each project, with varying levels of mitigation according to the risk level.

While the programs and projects sampled had individual risk management processes and tools, there was no common framework or methodology used to incorporate key program or project risks into the sector and departmental risk profiles. Further, aligning risk management activities to performance measurement could allow for more defined linkages between risks and the expected outcomes of programs.

Without a common framework or process for integrating key program and project risks, it may not be possible to capture a complete picture of all major risks, and efforts to prioritize risk management activities across the sector may be limited. Without anchoring risk activities to program outcomes, risk mitigation efforts may not be directly related to the objectives of programs.

Recommendation 4 (Medium Risk):

CMS should develop and communicate tools to support sector-level risk management activities that are aligned to strategic planning activities.

4.5 COMMUNICATION AND GUIDANCE

Communication on risks is in place in the context of the Integrated Planning and Reporting process. Outside of this process, there is limited guidance and communication to support risk management activities and build risk management capacity in the Department.

Communication and consultation with stakeholders is expected to take place at all stages of the risk management process. While the process lead initiates the cycle with a formal call-out for information, continuous exchanges ensure that the information is accurate and consistently used across the organisation, and guidance can be provided in a timely fashion. A consultative approach helps establish the context appropriately, ensures that the interests of stakeholders are understood and that risks are adequately identified.

The Integrated Planning and Reporting (IPR) process is the main vehicle for gathering and integrating risk information across the Department. The process is managed through a formal call-out from CMS to sectors, which includes templates to be used along with general instructions on submitting the information. Sectors gather information across branches and programs, and submit their consolidated information to CMS, who in turn develops the Department's Corporate Plan. CMS communicates with sectors during the development of the Corporate Plan, including in the development of the Corporate Risk Profile and mitigation strategies.

However, there is limited guidance provided to sectors, apart from the IPR templates, or outreach to support risk management practices outside of the IPR process. Sectors demonstrated a lack of awareness of the Department's risk management framework, including the expectations for risk management activities to be performed by sectors. They indicated they were not clear on the Department's drivers for risk management and the process through which information is incorporated into the Corporate Risk Profile. Sectors also noted that they generally did not have the knowledge or capacity to perform risk management at the sector level.

Further, there is no systematic and continuous process to communicate risk management activities and priorities across the Department, whether horizontally or vertically. Beyond the Corporate Plan and the annual IPR cycle, risk information – such as the results of risk mitigation activities or results of any environmental scanning performed at the departmental level – is not communicated to sectors.

Without proactive and sufficient guidance and communication on risk management expectations, sectors may not consistently apply a common risk management framework. The absence of a continuous feedback loop between sectors and CMS could also hinder the Department's ability to incorporate risk information into strategic planning activities.

Recommendation 5 (Medium Risk):

CMS should develop formal risk management guidance for sectors, and develop an engagement plan to ensure the guidance is understood and commonly implemented.

4.6 CONTINUOUS IMPROVEMENT

A forum is in place for sectors to discuss risk management and lessons learned. However, continuous improvement is not embedded in risk management practices, and there are limited opportunities for building risk management capacity in the Department.

An effective risk management process should be dynamic, iterative, responsive to change, and incorporate good practices and lessons learned. Organizations should develop and implement strategies to improve their risk management operations, including improving risk management capacity, providing opportunities for training, sharing good practices and knowledge, and applying lessons learned over the lifecycle of the risk management process.

Sector Planning Working Group meetings, led by CMS through the Corporate Services Network and composed of planners from each sector, were identified as a forum for sharing risk management information. These meetings are held on a recurring basis and provide an opportunity for sector planners to discuss the IPR process with CMS. The Working Group holds meetings regularly in alignment with IPR timelines, including an IPR post-mortem meeting after each planning cycle. However, the depth of discussion around risk management was not supported by documentation or meeting agendas, and there is no process to ensure lessons learned in the post-mortem meetings are implemented in the next planning cycle.

In addition, there is no formal process to ensure risk information and risk management processes are reviewed and updated on a regular cycle across the Department. It should be noted, however, that since the time of the audit, CMS has undertaken a significant review of its risk management processes and tools, and how they might be more integrated into the IPR cycle. The review is supported by a detailed plan with milestones. CMS is encouraged to implement and periodically evaluate this new improvement initiative.

Continuous improvement and capacity-building efforts could be further strengthened through additional training for those responsible for risk management. As ample training opportunities exist within the public and private sectors, risk leads could benefit from additional awareness of available training, which could help to build a robust risk culture across the Department.

Without opportunities for continuous improvement, the Department's ability to address emerging or changing risks could be limited, and its risk management capacity may not mature. A lack of a process for regularly reviewing and updating risk management activities may hinder the Department's ability to respond to a changing environment and operational needs.

Recommendation 6 (Medium Risk):

CMS should implement a process to review ISED's risk management practices annually, promote learning and development opportunities, and actively share good practices and lessons learned across the Department.

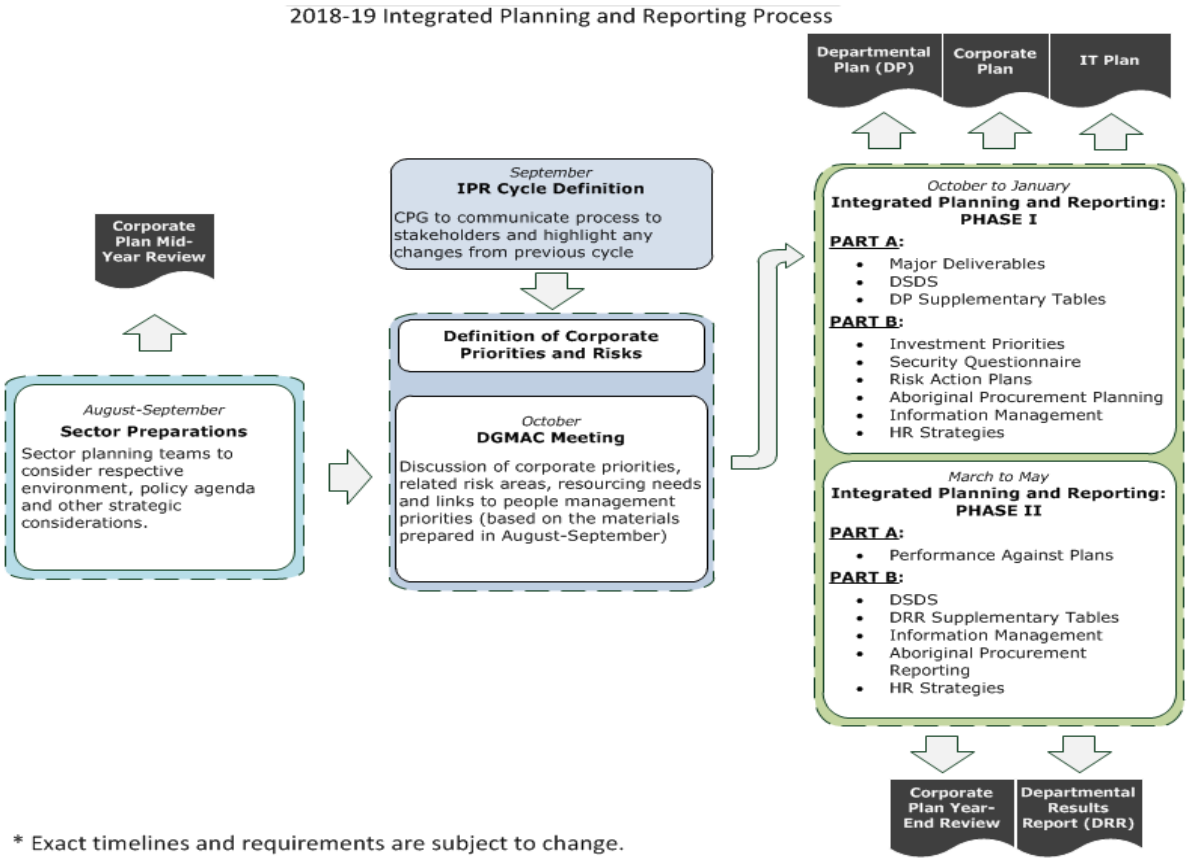
4.7 MANAGEMENT RESPONSE AND ACTION PLAN

The findings and recommendations of this audit were presented to the Corporate Management Sector. Management has agreed with the findings included in this report and will take action to address all recommendations by March 31, 2020.

5.0 CONCLUSION

Risk management activities are taking place at the corporate, sector and operational levels. However, the Department would benefit from more attention to risk management, supported by more formal processes, additional documentation, and regular monitoring at the corporate and sector levels. The Department would also benefit from more guidance and communication from the corporate function to support sectors' risk management practices.

APPENDIX A: INTEGRATED PLANNING AND REPORTING PROCESS



APPENDIX B: AUDIT CRITERIA

Audit of the Integrated Risk Management	
Audit Criteria	**Sub-Criteria**
1. The Department has established and implemented effective governance processes to support integrated risk management throughout the Department.	1.1 Roles, responsibilities, and accountabilities related to risk management are defined, updated, and communicated.
	1.2 Risk management is integrated in the Department's planning and reporting cycle.
	1.3 Risk management results are communicated in a timely manner to support informed decision-making.
Risk Management	
2. There is a risk management framework with processes and tools to identify, monitor, and mitigate risks.	2.1 The Department's corporate risk management processes are defined and communicated.
	2.2 Strategic and operational risk-based planning tools are in place and are used consistently to support processes.
	2.3 Effective sector-level and functional area processes are in place to identify, mitigate and monitor risks.
	2.4 A process is in place to integrate Sector risk profiles in the Department's Corporate Plan.
	2.5 Mechanisms for communication and guidance on risk management activities exist throughout the organization.
Internal Controls	
3. Innovation and continuous improvement are embedded in risk management practices.	3.1 Risk information and processes are reviewed and updated on an ongoing basis.
	3.2 The department and sectors actively participate in sharing of good practices and lessons learned with internal and external stakeholders.
	3.3 Training opportunities are promoted and mandated for staff in applicable roles.

APPENDIX C: AUDIT SAMPLE

Functional Areas	Selected Programs
Policy Analysis & Advice	• Entrepreneurship Policy • Business Policy and Analysis
Programs (Grants & Contributions)	• Futurpreneur • Economic Development in Northern Ontario (NODP) • Canada Foundation for Innovation • Canada Small Business Financing Program
Regulatory, Compliance & Enforcement	• Spectrum and Telecommunications • Competition Law Enforcement and Promotion • Federal Incorporation
Research & Development	• Communications Technologies, Research and Innovation
Project Management	• Data Centre Consolidation / Workload Migration (WLM) • FedNor Client and Office Management Solution (COMS) • Procurement Process Modernization Initiative • GCDocs

APPENDIX D: CORPORATE RISK MANAGEMENT PROCESS