Office of the
Auditor General
City of Ottawa

Audit of Enterprise Risk Management

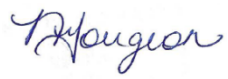
June 2022

Table of Contents

Acknowledgement

The team responsible for this audit was comprised of Rhea Khanna from the Office of the Auditor General and Samson (external consultant), under the supervision of Joanne Gorenstein, Deputy Auditor General and my direction. My colleagues and I would like to thank those individuals who contributed to this project, and particularly, those who provided insights and comments as part of this audit.

Respectfully,



Nathalie Gougeon, CPA, CA, CIA, CRMA, B. Comm
Auditor General

Introduction

The Audit of Enterprise Risk Management (ERM) at the City of Ottawa (or "the City") was included in the 2022-2023 work plan of the Office of the Auditor General (OAG), approved by City Council on December 3, 2021.

Background and context

The City is a large and complex municipality responsible for delivering a multitude of services to Ottawa residents and its visitors. It is important that the City has processes in place to identify, manage, and mitigate risks to the achievement of the priorities set out in its 2019 – 2022 Strategic Plan and its Official Plan.

ERM involves establishing enterprise-wide processes and practices to identify, assess, mitigate, monitor, and report on risks to the successful achievement of organizational objectives. Successful ERM programs ensure consistent and regular risk management activities throughout the organization and support strategic and operational decision making.

ERM within the City is governed by an ERM Policy ("the Policy"; last updated in 2019) and a supporting ERM Framework ("the Framework"; developed by Corporate Business Services based on the conceptual ERM Framework approved by Council and dated September 25, 2011). The Policy and Framework describe the general expectations for risk management activities across the City, identify key roles and responsibilities in the risk management process, and provide some risk management tools to ensure that risks are assessed and managed in a consistent manner throughout the City.

ERM practices at the City have evolved since the development of the Framework. In 2016, the decision was made to adopt a decentralized model whereby each department would be responsible for managing its own risks. Notwithstanding risks at the operational, project or program level, there are three main levels of risks considered as part of the Framework: departmental, horizontal, and corporate. Currently, each General Manager (GM) is accountable for departmental risks and risk management practices within their departments. Department-level activities are supported by the Business Support Services (BSS) unit within each department.

Departmental, horizontal, and corporate risks are reviewed as part of an annual cycle. Following the annual update of departmental risks, the Innovative Client Services Department (ICSD) coordinates a collaborative exercise with BSS risk leads to review

departmental risks to identify any horizontal risks (i.e., risks that are identified by more than one department). Horizontal risks are analyzed for collective mitigation opportunities and to determine whether any require escalation to the Senior Leadership Team (SLT) as new corporate risks. As part of the evolving risk management practices, horizontal risk trends are now provided to SLT annually to inform future risk reviews.

ICSD also plays a coordination role with departments to identify corporate risks annually, and departments may also identify corporate risks during their departmental risk process.

Audit objective and scope

The objective of this audit was to provide reasonable assurance regarding the City's ERM program. More specifically, the audit assessed whether:

- the City's approach to ERM enables effective risk-based decision making;
- ERM processes and practices have been established, aligned to the Framework and Policy and are being consistently applied across all departments; and
- the City has a robust risk management culture that encourages ongoing risk identification and management.

The audit focussed on risk management activities performed at the corporate and departmental level within the City by employees, members of the management team and City Council (or "Council") members. Areas of focus included:

- Governance and oversight;
- Implementation of ERM processes;
- Risk monitoring, reporting, and decision making; and
- Risk management culture (focused on awareness of processes, responsibilities, attitudes, training and support from senior management).

The audit covered the period from January 1, 2019 to December 31, 2021.

The audit did not assess project or program specific risk management activities. Further, it was our understanding that the COVID-19 pandemic impacted ERM processes and activities within our scope period. We adjusted our audit procedures to review and assess alternative activities and work products developed in response, where appropriate. Please see **Appendix 1** for detailed audit criteria.

Conclusion

Based on the work conducted, we found that the City has an ERM program in place supported by an ERM Policy and Framework. In many aspects, the City is further along in their ERM maturity than other jurisdictions in Ontario. At the corporate/City level, there are sound and robust processes in place to support the identification and management of the most significant risks to the organization and those which are horizontal across several departments. These processes support the development and update of an annual Corporate Risk Review which is provided to the SLT.

The audit further concluded that there are a number of opportunities for improvement, which should be addressed to strengthen the current practices across the City and mature the overall program. In general, these opportunities involve clarifying roles, responsibilities, and processes in the Policy and Framework; ensuring that the Policy and Framework requirements are being consistently adhered to at the departmental level; and providing for a centralized oversight and challenge role that will ensure the quality and consistency of risk management activities across the City. Additional opportunities to improve the ERM program were outlined in a letter provided directly to management.

Audit findings and recommendations

1. ERM Roles and Responsibilities

1.1 Further Defining Roles and Responsibilities

The Policy defines roles and responsibilities, at a high level, to support the decentralized model of risk management. This model recognizes that "the management of risk is a shared responsibility at all City levels"[1]. The Framework assigns GMs responsibility for managing and overseeing risks within their departments and specifically outlines the role of departmental BSS groups, management and all employees related to risk management.

The Framework, which supports the Policy, has not been updated since 2012. We noted that the Framework does not outline the specific roles and responsibilities in the context of the corporate and departmental level risk management processes. For example, the Framework does not outline:

- SLT's role in the review and approval of escalated corporate risks and mitigation strategies.
- ICSD's role in the corporate and horizontal risk management processes.
- Expectations for departmental management in developing their risk registers and mitigation strategies.
- Roles and responsibilities of risk owners in implementing risk mitigation strategies, monitoring, and reporting on the risk throughout the year.

A key requirement of a strong ERM program is to enable a consistent and regular process of identifying, assessing, and managing significant risks for the organization. It is therefore important that the roles and responsibilities mentioned above are clearly described (i.e., who, what, when, why and how) to ensure consistency in the risk management activities across the City and from year to year.

We understand that management has plans to review and update the Policy and Framework in the near term.

1.2 Informing Council

Council's role relative to ERM has been established as the approval of the ERM Policy and Framework. Consistent with the approach approved by Council in December 2013

[1] Enhanced Risk Management (ERM) Framework; Corporate Business Services, 09/25/2011.

as part of the Revision to Enhanced Risk Management Policy report (ACS2013-CMR-OCM-0023), Council is made aware of risks through information presented to them in Submission Reports (focused on specific projects, issues or topics) and, in some instances, through initiative specific reporting. However, members of Council are not currently informed of significant risk exposures facing the City as identified in the Corporate Risk Review (i.e., in a consolidated manner to get a global picture and understanding of various risks, their rankings, their interdependencies, and the status of risk mitigation strategies).

Council approves the high-level vision and direction for the City in its Strategic Plan which contains a number of priorities. To guide their ongoing decision making, Council should be aware of the significant risks facing the City, as identified within the ERM process, that may affect the achievement of its priorities.

1.3 ERM Training Program

Due to the decentralized risk management model, there are stakeholders with risk management responsibilities in each department, including: BSS representatives, risk Subject Matter Experts (SME) within service areas, the Departmental Leadership Team (DLT) and the GM. Each of these stakeholders must have a baseline and consistent understanding of the City's ERM process and their role within it.

The audit confirmed that there are a number of training materials and modules available to employees that were developed to support the initial Framework. There is, however, no mandatory risk management training program directed to those with specific risk management responsibilities to ensure there is a consistent understanding of risk management principles and the expectations of the City. Further, our audit did not identify any circumstances where organized risk management training is being provided at the departmental level.

Additionally, because of their lack of involvement in the ERM program, Council members do not necessarily have a fulsome understanding of risk management principles and the City's ERM program.

Conclusion

The City has an ERM Policy and Framework which are key elements in establishing and maintaining an ERM program that supports consistent City-wide risk management activities and effective risk-based decision making. There are several areas where the ERM Policy and Framework should be updated or strengthened, with appropriate training provided, to ensure roles and responsibilities are clearly understood.

Recommendation 1 – Clearly define roles and responsibilities in the Policy and Framework

The GM, ICSD, as part of the review and update of the Policy and Framework, should clearly define roles and responsibilities for risk management. This includes:

- Departmental management, ICSD and SLT's roles in the annual/ongoing risk management processes.
- Clear expectations for risk owners including responsibilities to implement risk mitigation strategies and regular reporting of the status of the mitigation activities and the impact on the assessed risks.

Management Response 1

Management agrees with this recommendation, and it is in the process of being implemented.

The GM, ICSD will update the ERM Policy and Framework to clearly define the roles and responsibilities of departmental management, ICSD, SLT and other key risks stakeholders. This work has already started, with SLT approving their updated roles and responsibilities respecting risk management on April 21, 2022.

Language will be added to specifically address expectations for risk owners and their responsibilities to implement risk mitigation strategies and report on the status of these activities and how they impact the assessed risks.

ICSD will complete the full update in Q2 2022 and communicate the updated policy and framework to the organization.

Recommendation 2 – Informing Council of corporate risks

The GM, ICSD, in conjunction with the City Manager and City Clerk, should determine what level of corporate risk information is recommended to provide to the next Council, including appropriate format, approach and frequency to enable Council members to consider such corporate risks as they are making strategic decisions.

MANAGEMENT RESPONSE 2

Management agrees with the recommendation.

The GM, ICSD will work with the City Manager and City Clerk to determine the appropriate format, approach, and frequency to report corporate risk information to City Council.

ICSD will start this work immediately and will prepare an approach and recommendation for the new Term of Council to consider by Q2 2023.

RECOMMENDATION 3 – MANDATORY RISK MANAGEMENT TRAINING

The GM, ICSD (or his/her delegate) should ensure that a mandatory risk management training program is developed and implemented` (initial and refresher training) for those individuals with specific risk management responsibilities. This training program could leverage the existing training modules and should be tailored to the various stakeholder groups involved in the risk management process.

MANAGEMENT RESPONSE 3

Management agrees with the recommendation.

The GM, ICSD will ensure that a mandatory initial and refresher risk management training program is developed and implemented for individuals with specific risk management responsibilities.

This training will leverage existing risk management training material and will address the learning requirements of key stakeholder groups involved in the risk management process.

The training will be in place by Q4 2022.

RECOMMENDATION 4 – RISK MANAGEMENT AWARENESS FOR COUNCIL

A risk management awareness/training program, specifically designed for the needs of Council, should be developed, and delivered to the next Council.

OAG RESPONSE 4

Once management has updated the Framework and Policy and has established the level of information to be provided to Council, the Auditor General has agreed to take

on the responsibility of providing risk management awareness training to the next Council to assist members in leveraging the ERM process in their decision-making. The Auditor General, in consultation with the City Clerk, will determine the most appropriate format and frequency for this training.

2. Risk Management Process

2.1 Corporate Processes

The City has implemented sound and robust risk management activities which are occurring at the corporate level (i.e., City-wide). These include:

- The Corporate Risk Review which is comprised of:
  - Assessments of the impact and likelihood of corporate risks.
  - Identification of the prime lead/risk owner.
  - Indication of the trend for the risk (increasing/stable/decreasing).
  - Identification of planned actions/mitigation strategies with target completion dates.
  - Reporting of progress on each risk mitigation strategy back to SLT.
- A semi-annual update of the Corporate Risk Review which is presented to the SLT.
- Through collaboration across the City, horizontal risks (which affect more than one department but do not meet the criteria to be escalated to the corporate risk register) are being identified and managed. This is achieved through an annual exercise of bringing departmental risk leads together to review and analyze the risks, identify common themes and interdependencies, as well as opportunities for collective mitigation. This exercise may also identify new corporate risks to be escalated to the SLT for consideration and direction.

2.2 Departmental Processes

To support departmental risk management activities, ICSD provides the tools and acts in a coordination role to enable meeting the expectations as outlined in the Policy and Framework. No specific oversight role for departmental activities has been assigned.

As part of the scope of our audit, we looked at the activities of three (3) departments over the past three (3) years. We were able to confirm that departments are producing annual risk registers. This annual exercise is exceeding the expectation outlined in the Framework, as it requires departments “to identify their top 3-5 risks, at a minimum, every other year".

Approaches taken across departments relative to their departmental risk management responsibilities are, however, inconsistent, which could result in not meeting the expected outcomes of the Framework. Examples include:

- Mitigation strategies repeated over several years with no evidence they have been implemented or changed the residual risk assessment.
- No risk mitigation strategies provided for some risks.
- Most mitigation strategies do not have planned completion dates to allow assessment of progress during the year.
- Not tracking risk mitigation strategies during the year.
- Not assigning owners to risks to implement and oversee the agreed upon mitigations.
- Not formally reviewing the mitigation progress during the year to assess the impact on the risk identified.

As noted in Observation 1.1, the Framework provides limited details of expectations related risk mitigation development, monitoring and reporting. Further, for the departments included in our scope, none had their own documented risk management procedures or guidelines to describe the GM's expectations of how to meet standards outlined in the Policy and Framework.

Without a centralized role to provide an oversight and challenge function, significant departmental risks may not be identified, assessed appropriately, and effectively mitigated and managed.

2.3 Fraud Risks

The risk of fraud and corruption is an inherent and significant risk for most organizations, including the City of Ottawa. Fraud can have many negative consequences including financial loss, impacts to employee morale, loss of public confidence and/or reductions in the efficiency or effectiveness of operations. Although it is not likely possible, or economically feasible, to completely eliminate all fraud risks, there are proactive approaches that can be taken to support the management of fraud risks. In many cases, these have been adopted by the City, primarily led by the Chief Financial Officer (CFO)/City Treasurer and the Financial Services Department (FSD).

Fraud is currently mentioned as one of many business process risks considered in the Framework; however, fraud risk has not been identified within the Framework as a specific risk category, which would ensure fraud-related discussions take place as part of risk management activities. Further, establishing the expectation to undertake a City-

wide fraud risk assessment would confirm a fulsome understanding of potential fraud risk exposures.

Conclusion

With the exception of a pause in ERM activities due to the pandemic (during which risk management activities were undertaken leveraging pandemic-related structures), the City has been performing an annual exercise to review risk registers, at both the corporate and departmental levels. The process at the City level involves oversight by the SLT and the identification of horizontal risks is functioning well.

Activities at the departmental level are not consistently applied. Furthermore, we have identified gaps in departmental activities such as: not identifying risk owners and not monitoring significant risks and progress of their associated mitigation strategies throughout the year. This suggests the need for some form of centralized oversight to ensure that a minimum standard is achieved across all departments.

Recommendation 5 – Establish centralized oversight

The City Manager should consider assigning additional authority and responsibility for ERM to ICSD or another centralized group (e.g., the Service Transformation Group), as owners to ensure all departments meet a minimum standard and consistency of expected risk management activities as set out in the Policy and Framework. This should include:

- Establishing a role in overseeing departmental risk management activities to ensure these activities achieve the outcomes intended from the Policy and Framework; and
- Providing an independent challenge function of the risk management output of departments given their City-wide visibility/perspective.

Management Response 5

Management agrees with the recommendation.

The City Manager will work with the GM, ICSD to consider assigning additional authority and responsibility for ERM to a centralized group as owners to strengthen oversight of departmental risk management activities to ensure all departments meet a minimum standard and consistency of risk management activities as set out in the Policy and Framework.

This will include an assessment of resource requirements, roles and responsibilities, and will be informed by the implementation of Recommendation 1 and Recommendation 7.

Implementation of this recommendation will be completed in Q3 2023.

RECOMMENDATION 6 – INTEGRATION OF FRAUD RISK WITHIN ERM

The GM, ICSD, in consultation with the CFO/City Treasurer, should establish expectations within the Framework, for the integration of fraud risks within ERM. Further, an enterprise-wide fraud risk assessment should be undertaken.

MANAGEMENT RESPONSE 6

Management agrees with the recommendation.

The GM, ICSD, in consultation with the CFO/Treasurer, will establish expectations within the ERM Framework for the integration of fraud risks in ERM processes and practices.

As part of the 2023 annual risk cycle (beginning in Q4 2022), departments will be asked to review fraud risks within their business processes and identify high, medium and low risks. This will be completed by Q2 2023. Once completed, the GM, ICSD, in consultation with the CFO/Treasurer, will determine an approach for an enterprise-wide fraud risk assessment.

An implementation plan for an enterprise-wide fraud risk assessment will be developed by Q4 2023.

3. Risk Appetite and Tolerance

3.1 Risk Appetite and Tolerance Levels

Risk appetite can be defined as “the amount and type of risk that an organization is willing to pursue or retain”[2]. Risk tolerance (which is complementary to risk appetite) is defined as “an organization’s readiness to bear the risk, after risk treatment, in order to achieve its objectives”[3]. The ERM Framework indicates that the Executive Committee “sets the City’s risk tolerance” and that Senior Management Committee members

[2] ISO Guide 73:2009 – Risk Management – Vocabulary; International Organization for Standardization.
[3] ISO Guide 73:2009 – Risk Management – Vocabulary; International Organization for Standardization.

"manage risks within their spheres of responsibility, consistent with the City' risk appetite".

Despite the Policy and Framework establishing the expectation, risk appetite and tolerance levels have not been established for the City or at a departmental level to guide the development of appropriate mitigation strategies.

Currently, risk appetite and tolerance levels are being inherently determined and communicated when SLT and DLTs review and approve risk assessments and related mitigation plans. For example, SLT will approve a risk mitigation plan that corresponds with their expectation of the City's risk tolerance.

Risk appetite and tolerance levels are important to establish to ensure that there is a common understanding of the City's acceptable and unacceptable risk exposures. Without expressed risk appetite statements and risk tolerance levels, each GM, manager and employee is applying their own standard to determining whether a risk is significant and acceptable for the City and/or their department.

Formally setting risk appetite statements and tolerance levels would further allow the City to pursue opportunities for which the risks are within specified tolerance levels or for which the opportunities outweigh the risks.

Conclusion

While the ERM Policy and Framework acknowledges the need for, and importance of, determining and communicating risk appetite and tolerance as part of an effective ERM program, these have not been formally established for the City.

Recommendation 7 – Establish risk tolerance levels

The City Manager, supported by the GM, ICSD should initiate an exercise to develop risk appetite statements and risk tolerance levels for the City and provide them to Council for approval to ensure appropriate resources are being allocated to mitigate risk where required and beneficial. Departments should utilize the established risk tolerance and appetite levels to determine where best to allocate their resources towards mitigation strategies.

Management Response 7

Management agrees with the recommendation.

At the Senior Leadership Team Meeting on April 21, 2022, the City Manager and SLT, supported by the GM, ICSD, approved the initiation of an exercise to develop risk

appetite statements and risk tolerance levels for the City and provide them to Council for approval to ensure appropriate resources are being allocated to mitigate risk where required and beneficial.

Planning for this exercise is underway, with the exercise expected to begin in Q3 2022 and completion estimated in Q2 2023.

Appendix 1 – About the audit

Audit objectives and criteria

The objective of this audit was to provide reasonable assurance regarding the City's ERM program. More specifically, the audit assessed whether:

- The City's approach to ERM enables effective risk-based decision making.
- ERM processes and practices have been established, aligned to the Framework and Policy and are being consistently applied across all departments.
- The City has a robust risk management culture that encourages ongoing risk identification and management.

Criteria listed below were developed based upon the City's ERM Framework and Policy and our understanding of current risk management practices.

	Governance and Oversight
1.1	The City has established an ERM policy and framework which clearly outline roles and responsibilities related to all activities involved in the systematic identification, assessment, mitigation, and management of risks within the City's tolerance levels.
1.2	The Senior Leadership Team (SLT) is involved in providing oversight of corporate risks and departmental risks, including monitoring key risks on an ongoing basis.
1.3	The City has a risk-aware culture where risk management activities are encouraged and supported by all levels of management and regular risk management training is provided to ensure awareness of risk management responsibilities and processes.
	Implementation of ERM Processes
2.1	An effective, consistent and systematic process is in place to support the development of the Corporate Risk Review, is leveraged in the strategic planning process, and is aligned to the Framework and Policy.
2.2	The risk management activities undertaken within departments are being completed in a consistent and systematic manner and are aligned to the Framework and Policy.

2.3	An effective process is in place to manage risks within the risk tolerance of the City and to escalate risks that may be above or approaching risk tolerance limits to the appropriate level of authority.
2.4	Centralized activities and oversight ensure that risk management activities in departments are being performed consistently and aligned to expectations across City departments.
2.5	All employees manage and mitigate risks within their areas of responsibility and escalate significant risks to the next level of authority.
	Risk Reporting, Monitoring and Decision Making
3.1	Current practices provide systematic, sufficient, and timely information, relating to significant risks that could impact the achievement of strategic priorities, to Council and SLT to enable risk management and decision making.
3.2	Mitigation strategies for significant risks are recommended/approved and monitored for implementation and effectiveness.

Scope

The audit focussed on risk management activities performed, at the corporate and departmental level within the City, by employees and Council members. Areas of focus included:

- Governance and oversight.
- Implementation of ERM processes.
- Risk monitoring, reporting, and decision making.
- Risk management culture (focused on awareness of processes, responsibilities, attitudes, training and support from senior management).

The audit covered the period from January 1, 2019 to December 31, 2021.

The audit did not assess project or program specific risk management activities. Further, it is our understanding that the COVID-19 pandemic impacted ERM processes and activities within our scope period. We adjusted our audit procedures to review and assess alternative activities and work products developed in response, where appropriate.

Audit approach and methodology

Audit staff performed the following procedures to complete this audit:

- Review and evaluate relevant policies, procedures, guidelines, and reports related to ERM.
- Interviews and walkthroughs with key personnel involved in risk management processes (corporate and departmental).
- Perform detailed reviews and testing of processes.
- Interviews with peer/comparable municipalities (benchmarking).
- Perform other analysis and tests, as deemed necessary.

Visit us online at www.oagottawa.ca

Follow us on Twitter @oagottawa

The **Fraud and Waste Hotline** is a confidential and anonymous service that allows City of Ottawa employees and members of the general public to report suspected or witnessed cases of fraud or waste 24 hours a day, seven days a week.

www.ottawa.fraudwaste-fraudeabus.ca / **1-866-959-9309**