



Office of the
Auditor General
City of Ottawa

Follow-up Report - Enterprise Risk Management Audit

SEPTEMBER 2025

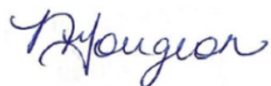
Table of Contents

Acknowledgement	1
Introduction.....	2
Background	2
Summary	2
Follow-up Findings and Recommendations.....	3

Acknowledgement

The team responsible for these follow-up procedures was comprised of Anna Koldewey from the Office of the Auditor General and Samson, an independent 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 work.

Respectfully,



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

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, waste or serious wrongdoing 24 hours a day, seven days a week.

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

Introduction

The Office of the Auditor General (OAG) Audit Charter requires the Auditor General to “follow up on engagement findings and confirm the implementation of recommendations or action plans and communicate the results”. Following the Audit of Enterprise Risk Management, the OAG performed follow-up procedures to confirm the steps taken to implement the recommendations.

Background

In June 2022, the OAG presented the [Audit of Enterprise Risk Management](#) to the Audit Committee. The overall objective of the audit was to provide reasonable assurance regarding the City of Ottawa’s (City) Enterprise Risk Management (ERM) program.

The audit found the City has an ERM program in place supported by an Enterprise Risk Management Policy (ERM Policy) and Enterprise Risk Management Framework (ERM Framework), with robust processes in place to identify and manage the most significant risks to the City. However, several areas were identified where the ERM program could be strengthened.

A total of seven (7) recommendations were issued as part of this audit report, one (1) of which was undertaken by the OAG. The key recommendations from the 2022 audit included:

- Clearly defining roles and responsibilities within the corporate and departmental risk management processes.
- Informing Council of significant corporate risks.
- Implementing a mandatory risk management training program for those with specific risk management responsibilities, including Council members.
- Establishing risk appetite and tolerance levels for the City.
- Integrating fraud risks within the ERM program and conducting an enterprise-wide fraud risk assessment.

By 2024, all but two (2) of the recommendations had been completed and the OAG had conducted follow-up procedures at that time.

In 2025, both recommendations #4 (ERM training for Councillors) and #6 (fraud risk management) were completed and the results of our follow-up work are outlined below.

Summary

The two outstanding recommendations stemming from the Audit of Enterprise Risk Management included the development of ERM training for Councillors (recommendation

#4) and the integration of fraud risk management (recommendation #6). Both have been deemed complete based on the work performed by the OAG.

As recognized in the audit, the City continues to mature its ERM program. Management has addressed all of the recommendations from the audit, and risk management is being embedded in discussions at leadership and Council tables. With a focus of continuous improvement, our follow-up work identified areas where management should focus its attention to ensure its ERM program supports effective decision making. This has resulted in additional follow-up recommendations.

Within the ERM program, Council's oversight role for ERM should be formalized, including how risk information is reported to Council. Additionally, there is an opportunity to provide more specificity to the City's risk appetite and tolerance statements to ensure consistent interpretation and application of these risk limits.

While the City completed its first organization-wide fraud risk assessment, there is currently no comprehensive Fraud Risk Management Program that establishes key fraud risk governance roles across the organization. Further, the fraud risk assessment conducted by management did not consistently identify specific fraud risk schemes and key control activities to mitigate the risks, which could undermine the City's effectiveness in detecting and responding to fraud.

Follow-up Findings and Recommendations

1. ERM Training for Councillors (Audit Report Recommendation #4)

Recommendation #4 of the Audit of Enterprise Risk Management indicated that a risk management awareness and training program, specifically designed for the needs of Council, should be developed, and delivered to the next Council. The OAG agreed to take responsibility for providing this training due to the lack of sufficient risk management expertise within City management at the time.

The OAG developed and delivered this training in April and May 2025 and, as such, the recommendation is deemed to be complete. The training materials developed were shared with the Risk Management Unit, within the City Manager's Office (CMO), for the provision of risk management training to future terms of Council and any new Councillors elected as a result of a by-election. During the preparation of the training program, several opportunities for improvement were identified as the ERM program continues to mature.

1.1 Council's Oversight Responsibilities for ERM

ERM within the City is governed by the ERM Policy and a supporting ERM Framework which describe the general expectations for risk management activities across the City,

identify key roles and responsibilities in the risk management process, and provide risk management tools to ensure that risks are assessed and managed in a consistent manner across the City.

1.1.1 Council's Role and Responsibilities

During the development of Council training on ERM, we noted that Council's responsibilities were not specified in the ERM Policy or Framework. Best practices indicate that key responsibilities for a governance body, such as City Council, should include:



In December 2013, Council delegated the responsibility for updating and approving the Policy and Framework to management. Following the Audit of Enterprise Risk Management, Council approved the process for reporting corporate risk information, as well as the City's risk appetite and tolerance statements. However, the lack of formalized roles and responsibilities could impact the effectiveness of Council's oversight of the City's risk management processes.

1.1.2 Risk Reporting to Council

In June 2023, the "[Enterprise Risk Management Program-Approval of Audit Recommended Actions Report](#)" was presented by Management to the Finance and Corporate Services Committee and approved by Council. This report outlined how corporate risk information will be communicated to Council going forward, focusing solely on corporate strategic risks. It also specified the timing of risk reporting to Council, in alignment with the Term of Council Priorities progress updates, which is to be provided at the midpoint and near the end of Council's term. Consequently, Council will receive updates on the top strategic risks to the City only twice during a term of Council.

Best practices recommend that audit committees/boards (or equivalent oversight bodies responsible for risk management) review the top risks at least annually to ensure they remain informed and can make timely decisions to manage risks effectively. Without regular reporting of top risks, Council may have limited visibility on the progress of existing risk mitigation and/or emerging risks, potentially impacting the City's ability to achieve its strategic objectives.

Although the City maintains a register of top corporate administrative risks, this is not shared with Council, which may result in insufficient attention to significant risks affecting the City's operations and services. While these corporate risks are not discussed at Council in the context of the ERM program, there are other ways this risk information is shared. For example, cybersecurity risks are discussed at the Finance and Corporate Services Committee, while provincial legislative changes are discussed at relevant committees, including the Planning and Housing and Public Works and Infrastructure Committees.

RECOMMENDATION 1: DEFINE COUNCIL'S RESPONSIBILITY FOR ERM OVERSIGHT

The Director, City Manager's Office should formalize Council's specific risk management responsibilities within the *Enterprise Risk Management Policy* and Framework. This should include a more frequent cycle of review of top corporate risks (both strategic or administrative) and the status of risk mitigation activities.

In conjunction with the City Clerk, these responsibilities should be reflected in the most appropriate committee's Terms of Reference.

MANAGEMENT RESPONSE 1

Management agrees with this recommendation.

The Director, City Manager's Office, will pilot an annual Enterprise Risk Management report to Council, covering aspects of the City's risk management practices, including strategic risks, administrative risks, mitigation activities and risk appetite and tolerance.

This pilot report will be brought to City Council in Q1, 2026.

Further, the Director, City Manager's Office will bring an administrative report to City Council recommending: an update to Council's risk management responsibilities, and an approach for a more frequent cycle of review of corporate strategic and administrative risks and related mitigation activities. Upon Council approval of this report, the Enterprise Risk Management Policy and Framework will be updated.

This administrative report will be completed in alignment with the governance activities of the 2026-2030 term of Council and the new City Strategic Plan (estimated completion in Q4, 2026 - Q1, 2027).

1.2 Risk Appetite and Tolerance

RISK APPETITE:

The types and amount of risk, on a broad level, that an organization is willing to accept in pursuit of its strategic objectives.

As part of addressing the recommendations from the Audit of Enterprise Risk Management, the City developed risk appetite and tolerance statements, outlining areas where the City is willing to accept and take on some risk and where the City has a low appetite for risk. These statements were approved by City Council in 2023. While management has indicated that the tolerance and appetite statements

are expected to be reviewed periodically (e.g. every term of Council), there is no defined schedule for their review and update. This can lead to outdated risk parameters that may not reflect decision-making needs or the current operational environment, especially if there have been significant changes in strategy, external factors, or operations.

For risk appetite and tolerance statements to be effective, they must be clearly defined to ensure consistent understanding and application in decision-making processes across the City. Currently, the statements use the qualitative terms such as "low," "medium," and "high" to describe the appetite for various risk types. While the 2023 report to Council provides additional guidance, for

example *"low tolerance indicates that the City is generally not willing to assume a particular risk"*, there is no clear definition of how these terms are to be interpreted or quantified. Without clearly articulated risk limits, the statements could be inconsistently applied leading to decisions made that are misaligned with the City's true risk appetite and tolerance levels.

RISK TOLERANCE:

The boundaries of risk-taking that an organization will not exceed.

Currently, the City's statements are framed only in the context of the organizational risk appetite and tolerance. However, it is important to recognize that different departments and services face varying levels and types of risks. As the City continues to build its risk capacity and maturity, each department should formally establish its own risk tolerance statements within the context of the overall organization's risk appetite and tolerance. This expectation is outlined in the City's ERM Policy which assigns General Managers the responsibility to define acceptable risk tolerance for the department level, in the context of the overall organizational risk appetite and tolerance set by Senior Leadership Team. Based on the information provided during our follow-up procedures, we understand this expectation has not yet been formally implemented. However, management has indicated that efforts are underway to address this.

Lastly, reporting on risk appetite is a best practice in risk management. This practice helps identify any risks that fall outside the defined risk appetite and tolerance levels, allowing management to escalate any risk exposure that approaches or exceeds these levels. Since the City is in the early stages of incorporating its risk appetite statements into decision-making processes, a reporting mechanism has not yet been established. This could be addressed by highlighting decisions that approach or exceed risk tolerance in the Risk Management Implications section of submission reports to Council.

RECOMMENDATION 2: ENHANCE CLARITY AND MANAGEMENT OF RISK APPETITE/TOLERANCE

To ensure a consistent understanding and application of the risk appetite and tolerance statements across the City, the Director, City Manager's Office should:

- implement a schedule for regular reviews and updates of risk appetite and tolerance levels to ensure they remain relevant for decision making;
- define risk limits to ensure they are consistently interpreted and understood across the organization; and
- communicate expectations for each department to develop risk tolerance statements specific to their environments while aligning with the overall corporate level appetite and tolerance levels.

Once this is complete, management should consider how decisions that approach or exceed the defined risk tolerance levels should be escalated and reported.

MANAGEMENT RESPONSE 2

Management agrees with this recommendation.

As part of the administrative report outlined in management response 1, the Director, City Manager's Office will recommend a schedule for regular review and updates of risk appetite and tolerance levels. This report will be completed in alignment with the new City Strategic Plan for the 2026-2030 Term of Council (estimated completion in Q4, 2026 - Q1, 2027).

Further, as part of ongoing continuous improvement activities, management will work with departments to define risk limits and risk appetite and tolerance statements specific to their environments, in alignment with the overall corporate appetite and tolerance. Management will also determine an appropriate escalation and reporting strategy for decisions that approach or exceed defined risk tolerance levels.

2. Fraud Risk Assessment (Audit Report Recommendation #6)

Recommendation #6 of the Audit of Enterprise Risk Management proposed that management integrate fraud risks into the ERM framework and conduct an enterprise-wide fraud risk assessment. This recommendation was deemed complete by management as of December 2024 as the Risk Management Unit had added fraud to its ERM risk categories and completed an enterprise fraud risk assessment resulting in a report titled “2024 Enterprise Fraud Risk Assessment Summary Report”; issued on January 10, 2025 to the City Manager’s Office.

As part of our follow-up procedures applied to the recommendation, we confirmed that the methodology used to develop the fraud risk assessment aligns with professional guidance and the exercise involved appropriate internal subject matter experts and departmental representatives. As management has completed the actions committed, this recommendation has been deemed complete by the OAG.

While we recognize that this first fraud risk assessment that was undertaken is a good starting point and will continue to strengthen over time, we have identified opportunities for improvement as the City’s Fraud Risk Management Program continues to mature.

When assessing the fraud risk assessment undertaken by the City, we used the ["Fraud Risk Management Guide – Second Edition,"](#) (the “2023 Guide”) published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the Association of Certified Fraud Examiners (ACFE) in 2023 as the authoritative guidance on fraud risk management.

2.1 Fraud Risk Management Program

The 2023 Guide defines a Fraud Risk Management Program as an organization’s overall set of processes and procedures, which includes the following components (as outlined in **Figure 1** below):

- Fraud risk governance;
- Fraud risk assessments;
- Preventative and detective fraud control activities;
- Fraud reporting mechanisms and fraud investigations protocol; and
- Systems for monitoring fraud risk management policies and procedures.

Figure 1: Ongoing, Comprehensive Fraud Risk Management Process

Adapted using the ACFE/COSO 2023 Fraud Risk Management Guide

Although the City has incorporated elements of fraud risk management within its [Fraud and Waste Policy](#) and [Employee Code of Conduct](#), it does not have a comprehensive, documented Fraud Risk Management Program. More specifically, we found there is no formal identification of key stakeholders, and their roles and responsibilities for fraud risk management.

Additionally, the City does not have a designated owner for fraud risk management at the City. The 2023 Guide recommends that an executive-level member of management, with the necessary authority and familiarity of the organization’s fraud risks and process-level controls, should lead fraud risk management activities.

While the City’s fraud risk assessment states that “*fraud risk exposure should be assessed periodically by the organization*”, without a comprehensive Fraud Risk Management Program, it is unclear how exactly this will be accomplished, how frequent and whether the responsibilities are well understood and subject to appropriate oversight. Additionally, to date, there has been no documented process for how fraud risk controls are to be designed, monitored, and tested to ensure these controls are effective in monitoring fraud risk across the organization. Furthermore, as the City’s *Fraud and*

Waste Policy would be a significant component of the Fraud Risk Management Program, it should be integrated into the overall framework. Without a defined Fraud Risk Management Program, the City may be ineffective in managing fraud risks across the City.

It should be noted that the City has established risk tolerance statements (as described in Section 1.2 above) as part of its ERM program, which outline the levels of risk the organization is willing to accept in various areas. However, the City has not included a specific tolerance statement related to fraud risk. Recognizing that it is impossible to eliminate all fraud risk, a clearly defined fraud risk tolerance statement provides a framework for understanding and managing the amount of fraud risk the City is willing to accept.

FRAUD RISK TOLERANCE:

The level of residual fraud risk that an organization is willing to accept that a fraudulent event or transaction will occur and not be detected in a timely manner.

RECOMMENDATION 3: ESTABLISH A COMPREHENSIVE FRAUD RISK MANAGEMENT PROGRAM

To provide an overall framework for the City to operate within, the City Manager should establish a comprehensive Fraud Risk Management Program, that will:

- assign overall responsibility for fraud risk management to a single executive (e.g. City Manager or General Manager, Finance and Corporate Services Department);
- formalize and document key stakeholders and their roles and responsibilities in the organization's Fraud Risk Management Program;
- define the City's fraud risk tolerance;
- establish an overall approach for the conduct of fraud risk assessments, including frequency;
- document the City's overall process for designing, monitoring, and testing fraud risk controls;
- integrate the City's *Fraud and Waste Policy*; and
- establish a process for formally assessing the effectiveness of the Program.

MANAGEMENT RESPONSE 3

Management agrees with this recommendation.

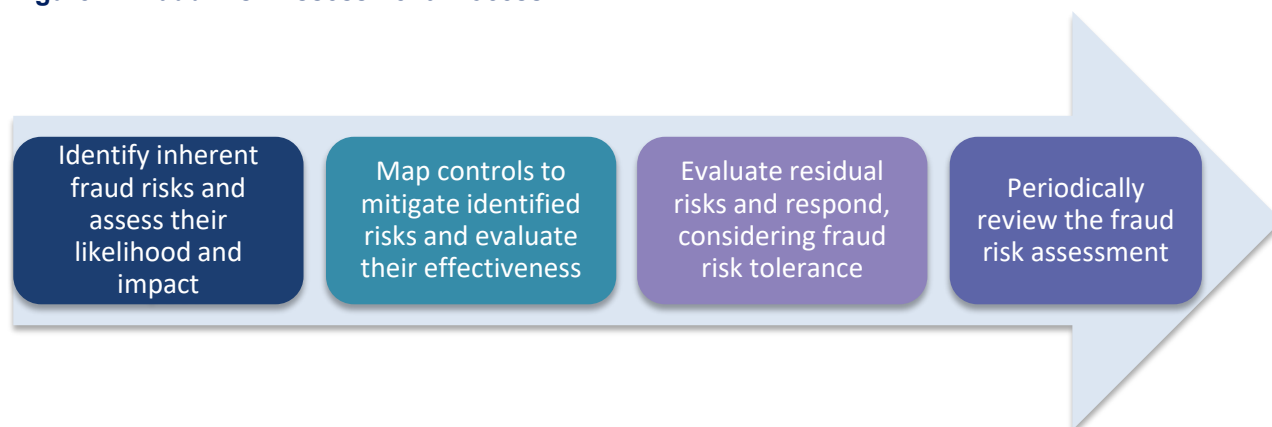
A Fraud Risk Management Program will be created in alignment with the existing Enterprise Risk Management Program. The City Manager, in conjunction with the General Manager, Finance and Corporate Services Department will work together to include the elements described in this recommendation into this program.

Management will confirm fraud risk governance by Q2, 2026 and the program will be created by Q2, 2027.

2.2 Fraud Risk Assessment

A comprehensive fraud risk assessment allows the City to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risk. A general fraud risk assessment process is illustrated in **Figure 2** below.

Figure 2: Fraud Risk Assessment Process



Adapted using the ACFE/COSO 2023 Fraud Risk Management Guide

As the City continues to mature this process, opportunities to strengthen the approach have been identified. Several of the opportunities noted below will support an overall Fraud Risk Management Program (as outlined in Section 1.1 above).

2.2.1 Identification of fraud schemes and risks

As input into the fraud risk assessment, the City's Risk Management Unit conducted research to identify and categorize global fraud risks. Individual departments had the opportunity to add or modify risk examples specific to their environment.

We noted that the fraud risk assessment documentation summarized potential fraud broadly rather than detailing those specific risks relevant to the City. For example, one

category of risk identified in the fraud risk assessment is "Procurement fraud," which is described as *"illegal acts such as bid rigging, kickbacks, fraudulent billing in the procurement process, manipulating bidding processes to favor certain vendors in exchange for bribes or other benefits"*. This type of description covers various behaviors and potential fraud schemes that could be perpetrated against the City, each with different levels of risk and requiring distinct control activities to mitigate the risk.

Without establishing fraud schemes/risks specific to the City, the most appropriate and efficient controls to mitigate the risks may not be identified and relied upon. This includes leveraging fraud risk schemes/trends identified through the Fraud and Waste Hotline.

2.2.2 Assessment of risk likelihood and significance

Assessing the inherent likelihood and significance of fraud schemes is a key principle identified in the 2023 Guide. The fraud risk assessment states at high-level that *"the general inherent risk for fraud is high, given the significant impact of financial loss, reputation/public confidence loss and inability to provide effective services."* However, it is unclear whether inherent risk was discussed or assessed during the fraud risk assessment process for specific risks as it was not documented in the summary report nor was this assessment included in the detailed fraud risk summary workbook.

INHERENT RISK: The level of risk that exists before any controls or mitigating actions are applied.

Without assessing inherent risk first, it is difficult for the City to identify areas requiring appropriate mitigating controls to ensure that the remaining risk is within its risk tolerance.

2.2.3 Identification and testing of existing fraud risk control activities

FRAUD CONTROL ACTIVITY:

A specific procedure or process intended to either prevent or detect fraud.

Ensuring that identified fraud controls are functioning properly requires ongoing compliance testing and regular reviews of risk factors and business processes. In the example of Procurement Fraud, the City has outlined several corporate controls, including the *Employee Code of Conduct*, *Finance 101 training*, *Internal Controls training*, *Our City Our Code Ethics training*, the *Purchasing Card Policy*, and the *Purchasing Card Procedure*.

Although the fraud risk assessment lists several fraud control activities for each identified fraud scheme, it does not consistently match specific controls with distinct fraud risks. As noted in the paragraph above, many of the control activities listed are general policies and expectations rather than concrete, actionable measures that would prevent and

detect fraud. In some cases, no specific control activity has been identified, indicating a potential overreliance on the high-level policies and corporate values and expectations as substitutes for targeted fraud mitigation controls.

Where specific fraud control activities are identified, it remains unclear whether they are subject to regular testing to confirm they are operating as designed. Without periodic assessments, the City cannot verify the operational effectiveness of these controls in order to rely on them and accurately assess the level of residual fraud risk the City faces.

This lack of clarity on how individual risks are mitigated and whether the associated controls are effective, could result in insufficient controls to mitigate the risk or overreliance on an ineffective control. Conversely, there could be fraud risks that are overcontrolled, meaning excessive resources could be allocated to fraud risks that fall within the City's fraud risk tolerance, once that tolerance is formally defined.

2.2.4 Response to residual fraud risks and continual assessment

The fraud risk assessment outlines an expectation that the assessment be refreshed periodically and that the results be shared with departments for review, action, and integration into ongoing risk management processes. However, it is unclear how often this will be done and how/with whom the results will be shared. Best practices indicate that senior management should regularly inform audit committees/boards (or equivalent oversight bodies responsible for risk management) about residual fraud risks identified in fraud risk assessments.

RESIDUAL RISK:
The amount of risk that remains after control activities are successfully implemented.

Additionally, the fraud risk assessment identified residual risk levels for each fraud risk category and indicates that action and/or increased monitoring is required for those assessed as medium or high risk. While some actions are identified, these suggestions are often general (e.g., “review, rationalize, and align the City's anti-corruption practices with industry leading practices”) rather than specific, actionable steps. A detailed action plan, with defined roles, responsibilities and timelines, for strengthening certain controls was not developed as part of the fraud risk assessment. This lack of clarity and accountability could result in corrective actions not being implemented or tracked.

Overall, while this first iteration of the fraud risk assessment was a good starting point, there is an opportunity to establish associated processes and improve the level of specificity of the analysis to support fraud risk management within the City.

RECOMMENDATION 4 – STRENGTHEN FRAUD RISK ASSESSMENT PROCESSES

As the fraud risk assessment process matures, the City Manager or the individual designated as responsible for fraud risk management should:

- increase the specificity of fraud schemes/risks applicable to the City;
- consistently assess inherent risk for each fraud scheme/risk that could be perpetrated against the City;
- identify and document specific control activities designed to mitigate those risks that have been assessed as above the City's risk tolerance; and
- establish a cycle to conduct periodic compliance testing, aligned with the Fraud Risk Management Program, of the identified key controls to evaluate their effectiveness.

MANAGEMENT RESPONSE 4

Management agrees with this recommendation.

This recommendation will be addressed in line with recommendation 3 and will be included as part of the maturity plan for the Fraud Risk Management Program.

RECOMMENDATION 5: ENSURE ACCOUNTABILITY AND IMPLEMENTATION OF FOLLOW-UP ACTIONS

To ensure accountability and effective implementation of responses to high residual risks, the City Manager or the individual designated as responsible for fraud risk management should:

- share the results of the fraud risk assessment with Council for review and action;
- establish and formalize an appropriate cycle for refreshing the fraud risk assessment and integrate results into ongoing risk management processes; and
- clearly outline roles, responsibilities, and timelines for follow-up/remediation actions relative to improved controls to ensure accountability and effective implementation. This should include regular reporting on the status of remediation actions.

MANAGEMENT RESPONSE 5

Management agrees with this recommendation.

As part of the pilot ERM report outlined in management response 1, the results of the most recent fraud risk assessment will be shared with Council in Q1, 2026.

The remainder of this recommendation will be addressed in line with recommendations 3 and 4 and will be included as part of the overall Fraud Risk Management Program.