For Action

Audit, Finance and Risk Management Committee – 2026 Enterprise Risk Management Update

Date: May 26, 2026
To: Audit, Finance and Risk Management Committee
From: Head of Audit, Risk and Compliance

Recommendations

It is recommended that the Audit, Finance and Risk Management Committee:

1. Approve the updated Toronto Transit Commission Enterprise Risk Management Framework (Attachment 1).

Summary

The Audit, Risk and Compliance Department (ARC) has been tasked with progressing the maturity of the Enterprise Risk Management (ERM) Program at the TTC and reports to the Audit, Finance and Risk Management Committee (the Committee) on the status of the ERM Program and changes in the organization's risk profile. The purpose of this report is to provide the Committee with a progress update on key ERM Program initiatives.

Key updates to the framework for 2026 include:

- Alignment with the Audit, Finance and Risk Management Committee Terms of Reference.
- Updates to the Roles and Responsibilities section.
- Clarifications on the Five-Step Risk Management Process.

Background and Analysis

The TTC is continuing to build its ERM Program with the goal of, *Building Resilience and Capacity to Manage Enterprise Risks and Threats* and providing the Committee with enhanced oversight to effectively manage key risks. ARC continues to focus on delivering and strengthening the foundational components outlined in its ERM Multi-Year Roadmap to ensure the long-term success of the TTC's ERM Program. Key developments include:

- Preparation to refresh the TTC's Key Enterprise Risk portfolio;
- Enhance the approach to capture and assess risks; and
- Analysis of technology solutions in collaboration with IT Services to support future risk monitoring and reporting.

TTC's ERM Framework

The TTC's ERM Framework is intended to guide the enterprise risk management process and has been developed by taking into account generally accepted risk management practices and standards including the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management Integrated Framework and ISO 31000. The document outlines a Five-Step process for risk management: identify, assess, respond, report and monitor and provides details on roles and responsibilities. The overall goal of the ERM Framework is to establish a systematic approach to identifying, managing and reporting risks and to enhance risk management capabilities within the organization.

As indicated in the TTC's ERM Framework it is the Audit, Finance and Risk Management Committee's responsibility to review and endorse the Framework including any changes on an annual basis. The ERM Framework is being provided to the Committee for review and approval and is included as Attachment 1 of this report.

Key Enterprise Risk Update

Key Enterprise Risk	
1. Capital Funding Requirements	6. Disruption
2. Cybersecurity	7. Governance and Decision-Making
3. Recruitment and Retention	8. Strategy Development and Execution
4. Financial Sustainability	9. Third Party Vendor
5. Public Safety and Transit Security	10. Worker and Customer Safety

In Q1 2026, ARC met with all Chief Officers (Key Risk Owners) to review the 10 Key Enterprise Risks. Discussions focused on validating the current risk level of each risk and key actions to mitigate exposures. The primary objective of this exercise is to fulfil the ERM function's monitoring responsibilities, while developing a standardized risk reporting structure. A summary report is currently under development and will be communicated upon completion in Q2 2026.

Key Enterprise Risk Refresh

ARC is preparing to collaborate with Executive Leadership and key stakeholders to refresh the current Key Enterprise Risk portfolio and further develop a comprehensive Enterprise Risk Inventory. The refresh of the Key Enterprise Risk inventory is an important step in advancing the TTC's ERM maturity as it will enhance the organization's capacity to identify and assess risks by providing a structured approach and repository of risk information. This will include risk categories, sub-risks, risk scores, key metrics and controls, and will facilitate an enhanced and adaptable approach to embed risk practices management across the TTC. This work aligns with the ERM Multi-Year Roadmap and is anticipated to conclude at the end of Q1 2027.

Diversity, Equity and Inclusion Matters

ERM supports TTC leadership efforts to continuously improve controls and integrate risk management into processes that drive the achievement of corporate goals and objectives, including equity, diversity, inclusion, and accessibility.

Innovation and Sustainability Considerations

ARC's Enterprise Risk Management Program contributes to innovation and sustainability by promoting continuous improvement in governance, risk management, and internal controls. Through its risk and assurance work, ARC helps identify opportunities for operational efficiencies, digital transformation, and process enhancements that support long-term organizational resilience.

Corporate Plan Alignment

ARC's independent risk stewardship and advisory support all five strategic directions of the TTC's Corporate Plan. The ERM Program facilitates a proactive, systematic, and organization-wide approach to identify, assess and respond to risks that may impact the achievement of the TTC's objectives as outlined in its Corporate Plan. By advancing the ERM Program, ARC strengthens the TTC's governance and strategic decision-making capabilities further equipping the organization to manage complex challenges, and support transformation and modernization initiatives.

Financial Impact

The development and execution of the ERM Program by ARC has no funding implications beyond the costs included in the 2026 Operating Budget approved by the TTC Board on January 7, 2026, and by City Council on February 10, 2026.

The Interim Chief Financial Officer has reviewed this report and agrees with the financial impact information.

Contact

Viraj Chandrakanthan, Head – Audit, Risk, and Compliance
viraj.chandrakanthan@ttc.ca

Attachments

Attachment 1 – TTC ERM Framework

Attachment 1

TORONTO TRANSIT COMMISSION
ENTERPRISE RISK MANAGEMENT FRAMEWORK

TABLE OF CONTENTS

INTRODUCTION

ENTERPRISE RISK MANAGEMENT AT THE TTC

The TTC's Enterprise Risk Management (ERM) Program is designed to provide additional attention to identify, assess, manage, and monitor risks within the TTC in order to enhance the outcome of the TTC's business objectives. This definition recognizes that risk management is not an exclusive exercise or function responsibility, and that risk management should be integrated into key processes and decision-making. The contents of this Framework will continue to evolve as the TTC's ERM Program matures over time.

This Framework has been developed by taking into account recommendations from generally accepted risk management practices and standards, including the Committee of Sponsoring Organizations (COSO) of the Treadway Commission Enterprise Risk Management Integrated Framework and ISO 31000.

VISION

The vision for ERM is to embed risk management into the TTC's governance, culture, and decision-making processes resulting in enhanced risk management capabilities throughout the organization. The underlying philosophy is that risk management is not an exclusive exercise or function. Rather, risk management is everyone's responsibility.

ERM FRAMEWORK GOALS AND OBJECTIVES

The overall goal of the TTC's ERM Framework is to enhance risk management capabilities within the organization. The underlying goals and objectives are to:

- Identify and understand key enterprise risks.
- Apply the ERM Framework to each key enterprise risk.
- Facilitate key enterprise risk reporting to management and the Audit, Finance and Risk Management Committee.
- Provide tools to assist with assessing risk, including identifying root causes and impacts.
- Convey the TTC's commitment to the regular review and continual improvement of this ERM Framework.
- Integrate ERM with the TTC's Corporate Plan and Business Planning activities.

GUIDING PRINCIPLES

The primary guidelines in effective risk management are as follows:

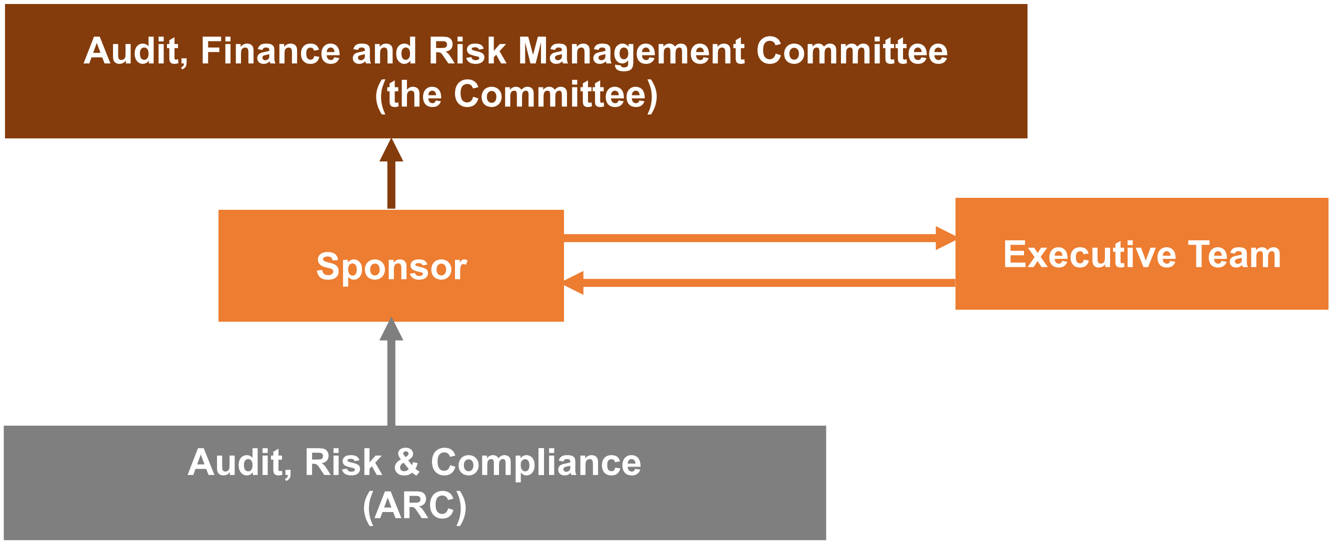
- **Risk management is everyone's responsibility:** The Board, all levels of management, and individual employees are responsible for understanding the principal risks in their areas of responsibility and for making effective risk management decisions.

- **Significant risks are identified and managed through an integrated approach:** A comprehensive, disciplined, and consistent approach to risk management will be ongoing and integrated with other risk management areas.

- **Continuous Improvement:** The ERM Program will be continuously improved to ensure that it reflects good industry practice, adds value to the business, and adapts to changes in strategic and business objectives. It will also recognize different stages of maturity in elements of the ERM Program.

GOVERNANCE

The governance structure of the ERM process is depicted below:



ROLES AND RESPONSIBILITIES

Audit, Finance and Risk Management Committee (the Committee)

The role of the Committee is to:

- Set the tone on risk management culture and awareness.
- Review and approve the TTC's ERM Framework, including any changes.
- Review the risk profile to ascertain the validity and management of enterprise risks.
- Request Risk Owners to attend meetings (as needed) to provide respective enterprise risk updates.
- Direct ARC to conduct risk-based reviews of the TTC's management and operations, and escalate risk related matters to the Board, as appropriate.

ERM Sponsor

The ERM Sponsor is a designated Executive who is accountable for ensuring the effectiveness of the ERM Program and champions adherence to the principles and requirements of this Framework across the organization. The role of the ERM Sponsor is to:

- Set an appropriate tone from the top that supports the effective implementation of the ERM Framework.
- Monitor ERM Program efforts and report ERM Program activities to the Committee.
- Support accountability and action.
- Provide ongoing guidance and input to the ARC Department on the TTC's enterprise risks.
- Communicating the 'tone from the top' and fostering an organizational culture that supports the integration of risk management throughout the TTC's business activities and strategy.

Executive Team

The role of the TTC's Executive Team is to:

- Identify and manage risks across the TTC and adhere to the ERM Framework, process, procedures, and Enterprise Risk Inventory.

- Be active sponsors and supporters of ERM Program activities and ensure adequate progress is being made on the achievement of desired control capabilities and timelines for mitigation.
- Manage and monitor risks within their areas, finalize mitigation plans as appropriate, and provide updates to the Committee periodically.
- Address mitigation strategies, control enhancements, additional actions required, and emerging risk considerations.
- Embed risk awareness and culture in day-to-day operations.
- Instill a culture of accountability for risk management activities.
- Allocate resources to help achieve intended risk mitigation efforts.
- Integrate risk management with other business planning, management activities, key processes, and decision-making.
- Prioritize the key risks to achieving strategic objectives.
- Address escalated risk issues.
- Collaborate to ensure a detailed Risk Analysis and Risk on a Page Summary Report is completed for each of their enterprise risks.

Audit, Risk, and Compliance Department (ARC)

The role of ARC is to:

- Provide ongoing input and support for the continuous improvement of the ERM Framework.
- Support Executive Risk Owners in the risk identification, assessment, and response process, and prepare and present ERM Program activities and results to the Executive Team and the Committee.
- Align the annual internal risk-based audit plan and internal audit activities with ERM risk assessment results as deemed appropriate.
- Provide independent and effective oversight challenges to departments.

All TTC Staff

The role of all TTC staff is to:

- Report risks at their source to their appropriate line-manager or delegated risk representative.
- Continuously learning about risk management.

TTC FIVE-STEP RISK MANAGEMENT PROCESS

All risks at the TTC should be assessed using the following Five-Step Risk Management Process to ensure risks are consistently evaluated and prioritized:

STEP 1: RISK IDENTIFICATION

Enterprise risks have impacts that could significantly affect the TTC's ability to achieve its corporate objectives and are identified by the Executive Team. ARC facilitates risk identification through a variety of means, including individual risk interviews with each Executive, an

Executive-level risk workshop, and/or by circulating a risk identification survey. These methods are designed to build consensus on the TTC's list of key enterprise risks.

In summary, the Executive Team participates in these activities:

- Identify the TTC's enterprise risks.
- Further evaluate enterprise risks to arrive at a prioritized list of key enterprise risks.
- Accept individual risk ownership and accountability to mitigate each risk, as assigned.

Risk identification is an ongoing process and results in the continual development of the Enterprise Risk Inventory and prioritized list of Key Enterprise Risks, which lay the foundation for the subsequent Risk Assessment activities.

STEP 2: RISK ASSESSMENT

Risk Assessment is the process of measuring the level of exposure that each risk presents to the TTC's objectives. Once the risks are identified, each Executive Risk Owner will complete a Risk Analysis for each of their risks.

The resulting analysis ensures that risk status as well as opportunities for risk mitigation are identified and clearly communicated.

The Risk Assessment Procedure provides guidance and outlines the process for evaluating both inherent and residual risk ratings, the effectiveness of controls, and appropriate treatment plans.

STEP 3: RISK RESPONSE AND TREATMENT

Once a residual risk score is established, a risk response and a risk treatment plan must be developed to bring the risk to its desired level.

The TTC uses four common risk response types as described below:

a. Transfer or Share the risk to/with another party through insurance or outsourcing.
b. Avoid the risk by choosing not to undertake the activity.
c. Mitigate the likelihood of occurrence and/or the impact as low as reasonably achievable through mitigation strategies.
d. Accept the level of risk established, recognizing that the cost of transfer or mitigation outweighs the benefits of doing so.

The risk level would be unacceptable if it is outside the TTC's risk appetite. For all such risks, a determination shall be made in consultation with the Executive Team and Executive Risk Owner for further treatment (i.e. risk treatment plan or rationale for acceptance).

STEP 4: RISK REPORTING

Regular reporting of risk information is critical to support a robust ERM process and enable the Committee risk oversight. Risk reporting is expected to be conducted semi-annually or more frequently, as required. Feedback provided in response to risk reporting should be evaluated and incorporated, whenever possible.

Risk Owners and Risk Stewards are responsible for reporting on risks within their areas of accountability and escalating where necessary through established management and governance forums. Risk reporting should present relevant risk information, highlight material changes, and support transparency and escalation at the appropriate levels of the organization.

STEP 5: MONITORING

Risks and mitigations must be monitored on an ongoing basis by Risk Owners. Changes to any element of the risk, including new incident information, changes to controls, decisions as to the risk treatment/priorities, and the completion of risk actions must be reflected by updating the Risk Assessment. All risk actions are to be tracked to completion.

On an annual basis, the TTC ERM Framework and Key Enterprise Risk portfolio will be reviewed to ensure they reflect leading practice, and any changes in strategic objectives.

RISK APPETITE

Risk appetite needs to be reviewed at regular intervals and approved by the Committee. Factors such as new technology, or changes in business strategy may require the TTC to reassess its overall risk portfolio and adjust its appetites accordingly.

ENTERPRISE RISK INVENTORY

The Enterprise Risk Inventory is the TTC's centralized inventory of enterprise risks and associated risk information. It captures key risk information, including risk categories, sub risks, risk ratings, key metrics and controls, and serves as the primary repository for enterprise risk documentation and analysis. The Inventory is updated as new risks are identified or when there are changes to the assessment of existing risks, and its ongoing maintenance and periodic refresh support a more integrated and adaptable approach to embedding risk management practices into business planning, decision-making, and operational processes across the TTC.

RISK TRAINING AND COMMUNICATION

A critical component of the TTC's ERM Framework is training and communication. Training and communication supports are available and designed to ensure that TTC leadership has adequate awareness and understanding of the TTC's risk management processes and their responsibilities for the mitigation and management of risk. Effective training and communication support the consistent application of the ERM Framework and related process, while reinforcing a healthy risk culture.

FRAMEWORK EXCEPTIONS

The Head of ARC must report any exceptions to this Framework to the Committee at the next scheduled meeting. Changes to the ERM Framework require the Committee approval.

REFERENCES

- Audit, Finance and Risk Management Committee Terms of Reference.
- COSO, 2017 and 2018 ERM Framework.
- ISO 31000.

APPROVALS AND REVISION HISTORY

Version	Date	Author(s)	Revision Notes	Review	Approval
V1	March 19, 2024	Director, ARC	ERM Framework V1	Head - ARC	Audit, Finance and Risk Management Committee
V2	March 24, 2025	Director, ARC	Annual Review & Inclusion of Vision	Head - ARC	Audit, Finance and Risk Management Committee
V3	May 26, 2026	Director, ARC	Annual Review & Revision to Roles and Responsibilities	Head - ARC	Audit, Finance and Risk Management Committee

APPENDIX I – GLOSSARY OF TERMS

#	Key Term	Definition
1.	Enterprise	Any organization established to achieve a set of objectives.
2.	Enterprise Risk Management	A proactive, holistic, organization-wide approach to identifying and managing risks as an interrelated portfolio to support an organization's strategic goals.
3.	Control	Any action taken by management, the Board, and other parties to manage risk and increase the likelihood that established goals and objectives will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that goals and objectives will be achieved.
4.	Control Owners	An individual who is responsible for identifying and managing, processes, activities, and systems used to manage risks.
5.	Likelihood	The probability or chance that an incident and its associated outcome will occur.
6.	Impact	The effect, outcome, or consequence of a risk occurring.
7.	Inherent Risk	The risk that exists as part of the very nature of a process, activity, item, or object before considering the presence of controls and mitigating measures.
8.	Risk Appetite	The amount and type of risk that the organization is willing to pursue or retain.
9.	Risk	The possibility of an event occurring, which will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood[1].
10	Residual Risk	The risk remaining after controls or mitigating actions have been put in place.
11.	Risk Management	The process of identifying, assessing, responding, reporting and monitoring risks.
12.	Risk Owners	A Chief Officer who is ultimately accountable for managing a risk exposure. In managing the risk, they are responsible for managing their own controls, delegating responsibilities to members of their team and working closely with Control Owners and Risk Stewards.
13.	Risk Score	The assessed level of inherent risk or residual risk for each risk, is determined by applying the guidelines set out in the Risk Assessment Procedure.
14.	Risk Stewards	Designated subject matter experts or functions who have oversight responsibility for a specific type of risk, including the establishment of enterprise-wide policies and standards.

[1] Definition as per The Institute of Internal Auditors (IIA)