For Action

Audit, Risk and Compliance – Enterprise Risk Management Update

Date: March 19, 2024
To: Audit & Risk Management Committee
From: Deputy Chief Executive Officer

Summary

The Audit & Risk Management Committee Terms of Reference establishes that the Committee has oversight responsibility for Enterprise Risk Management (ERM). In 2023, the need was identified to re-establish a robust TTC ERM Program to support Executive Leadership decision-making and enable the Audit & Risk Management Committee to carry out its mandate. The Audit, Risk and Compliance (ARC) Department developed an initial Roadmap to facilitate this process and delivered all planned 2023 foundational items.

This report provides a detailed overview of progress made, including the completion of a comprehensive ERM Framework, identification by the TTC Executive Team of the organization’s Top 10 Key Enterprise Risks and the development of the 2024 ERM Roadmap. These actions will continue to build the maturity of the program and enable regular risk reporting at the Audit & Risk Management Committee.

Recommendations

It is recommended that the Audit & Risk Management Committee:

1. Approve the TTC’s Enterprise Risk Management Framework (Attachment 1).

2. Receive the list of Key Enterprise Risks (Attachment 2) and 2024 Enterprise Risk Management Roadmap (Attachment 3) for information.

Financial Summary

The facilitation by ARC to re-establish an ERM Program at the TTC has no funding implications beyond the costs of the Audit, Risk and Compliance Department that were included in the 2024 Operating Budget approved by the TTC Board on December 20, 2023, and by the City Council on February 14, 2024.

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

Equity/Accessibility Matters

The enterprise risk management advisory work of the ARC Department supports TTC leadership efforts to continuously improve controls and integrate risk management into processes that drive the achievement of corporate goals and objectives, including accessibility, diversity and inclusion.

Decision History

ARC's facilitation of the re-establishment of the ERM Program and the details of its 2023 ERM Roadmap were considered by the Audit & Risk Management Committee on November 14, 2023.
Audit, Risk and Compliance – 2023 Audit Plan Status Update

Issue Background

The Audit & Risk Management Committee assists the TTC Board in fulfilling its oversight responsibilities in several areas including audits, a system of internal control, compliance with laws and regulations, and enterprise risk management activities.

While the TTC Executive Team is accountable for enterprise risk management, ARC can support its efforts to oversee and drive risk management activities by serving in a risk advisory capacity.

Comments

Year in Review – 2023 ERM Roadmap

In 2023, ARC delivered on all milestones set out in its 2023 ERM Roadmap. Specifically, ARC:

- Engaged a third-party consultant to provide program recommendations and conduct a current state assessment.
- Facilitated a risk identification workshop with the Executive Team to establish a list of the Top 10 Key Enterprise Risks for the TTC.
- Conducted benchmarking and developed an ERM Framework to facilitate a consistent process for managing risk across the organization.
- Hired four senior advisors to support program development and implementation.
- Arranged risk training for the Executive and Audit & Risk Management Committee on basic risk principles and leading industry practices.
- Created a preliminary TTC risk universe.

TTC's ERM Framework

The overall goal of an ERM Framework is to establish a systematic approach to identifying, managing and reporting risks, and to enhance risk management capabilities within an organization. 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 (COSO) of the Treadway Commission Enterprise Risk Management Integrated Framework and the ISO 31000. The document outlines a five-step process for risk management: identify, assess, respond, report and monitor, as well as providing details on roles and responsibilities.

The TTC ERM Framework guides the frequency of risk management activities, including a cadence of risk reporting to the Audit & Risk Management Committee on a semi-annual basis. Executive Risk Owners will report on enterprise risks, progress made towards risk reduction, risk trends and overall progress on the ERM Program.

As indicated in the TTC's ERM Framework, it is the Audit & Risk Management Committee's responsibility to review and approve the Framework, including any changes on an annual basis. In line with this requirement, the Framework will be brought forward to the Audit & Risk Management Committee annually to ensure continual alignment with the TTC's business needs, risk appetite, industry best practices and emerging risks. Ongoing review and evaluation of the ERM Program is an important part of the TTC's continuous improvement efforts. The ERM Framework is being provided to the Audit & Risk Management Committee for review and approval and is included as Attachment 1 to this report.

10 Key Enterprise Risks – Workshop Results

In 2023, Key Enterprise Risks were identified and assessed by the Executive Team through an Executive Risk Workshop facilitated by a consultant. The workshop involved group discussion about the nature of significant risks impacting the TTC, root causes and existing controls, and was followed by a voting process. Each Executive voted on the likelihood of the risk materializing, what the impact on the organization would be, the speed by which it would happen (velocity), and management's current preparedness to respond. The result was a prioritized list of 10 Key Enterprise Risks that provide an important starting point for the ERM Program. This prioritized list of risks focuses the efforts of the organization, its resources and the Audit & Risk Management Committee's oversight on the risks that matter.

The list of Key Enterprise Risks is shown below.

#	Risks
1	**Financial sustainability**
2	**Capital funding requirements**
3	**Recruitment and retention**
4	**Worker and customer safety**
5	**Public safety and transit security**
6	**Governance and decision making**
7	**Cybersecurity**
8	**Disruption risk**
9	**Strategy development and execution**
10	**Third party vendor risk**

The workshop revealed that financial sustainability and capital funding requirements, the major root cause of which was inadequate and unpredictable funding, coupled with human resource challenges in recruiting and retaining talent, were major concerns for the Executive Team. For the remaining risks, including worker and customer safety, public safety and transit security, cybersecurity, disruption etc., the Executive Team perceived that controls existed but that work needed to be done to ensure controls are adequate and tested for effectiveness.

Executive Risk Owners will document risk response plans resulting in detailed summary reports called "Risk on a Page" for all 10 risks. The full risk matrix that plots each risk at the intersection of its inherent risk score and its management preparedness score is shown in Attachment 2.

2024 ERM Roadmap – Next Steps

The 2024 ERM Roadmap identifies the next steps for the current year, which are designed to further the program's maturation to a desired future state based on consultant recommendations. The Roadmap identifies key actions as detailed below.

Hub and Spoke Model – ERM Integration: A hub and spoke model is being explored to enable full integration of the ERM Program. The hub represents the central ERM function and is connected to the spokes representing local department level risk champions.

As a part of this strategy, considerable time and energy in 2024 will be devoted to collaborating with TTC's various departments to arrive at a process that links key enterprise risks to the interconnected operational level risks, with the ultimate aim of encouraging integrated risk discussions. A key focus will be identifying risk champions within operational risk areas to support risk management activities and drive further integration into departmental processes.

Pilot Project: In 2024, one key enterprise risk and a corresponding sub-risk will be fully assessed and reported on by the Executive risk owner in collaboration with a department risk champion. This will help to establish the link between operations and central ERM in a concrete way, and illustrate the relationship of aligned risk responses, metrics and measures.

ERM Policy*:* An ERM Policy that articulates the organizational vision for risk, and a risk philosophy that embodies the results of its hub and spoke work, will be developed. The Policy will articulate how ERM processes are integrated with strategic decision-making and aligned with operational risk management.

Risk on a Page: The completion of risk response plans will be guided by using a risk reporting template – Risk on a Page. Preparation of Preliminary Risk on a Page reports for all 10 Key Enterprise Risks is targeted for the end of 2024.

Risk Appetite: A Risk Appetite Framework will be developed based on statements as to how much risk the TTC is willing to assume concerning each of the Key Enterprise Risks articulated by the Executive Team. A Risk Appetite Framework will enable the

Audit & Risk Management Committee and the TTC to make informed decisions that are consistent with the organization's goals.

Enterprise Risk Inventory: An Enterprise Risk Inventory will be developed to serve as a repository for risk information. It will include main risks, sub-risks, risk scores and response plans.

Year-End Reporting: A year-end update report that measures and reports progress against the stated 2024 ERM Roadmap deliverables will be provided to the Audit & Risk Management Committee.

Conclusion

The completion of the foundational first steps sets the stage for the re-establishment of a robust ERM Program within the TTC. The ultimate goal will be the formal adoption of a systematic process for risk identification, assessment and reporting that will allow the Audit & Risk Management Committee to carry out its mandate for ERM as identified in its Terms of Reference.

Contact

Viraj Chandrakanthan, Head – Audit, Risk and Compliance
416-393-2030
viraj.chandrakanthan@ttc.ca

Signature

Bruce Macgregor
Deputy Chief Executive Officer

Attachments

Attachment 1 – ERM Framework
Attachment 2 – Top Risk Workshop Results
Attachment 3 – 2024 ERM Roadmap

Attachment 1

TORONTO TRANSIT COMMISSION ENTERPRISE RISK MANAGEMENT FRAMEWORK

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.

ERM FRAMEWORK GOALS AND OBJECTIVES

The TTC's ERM Framework's overall goal 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 & 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 TTC's Corporate Plan.

ERM GUIDELINES

The primary guidelines in effective risk management are as follows:

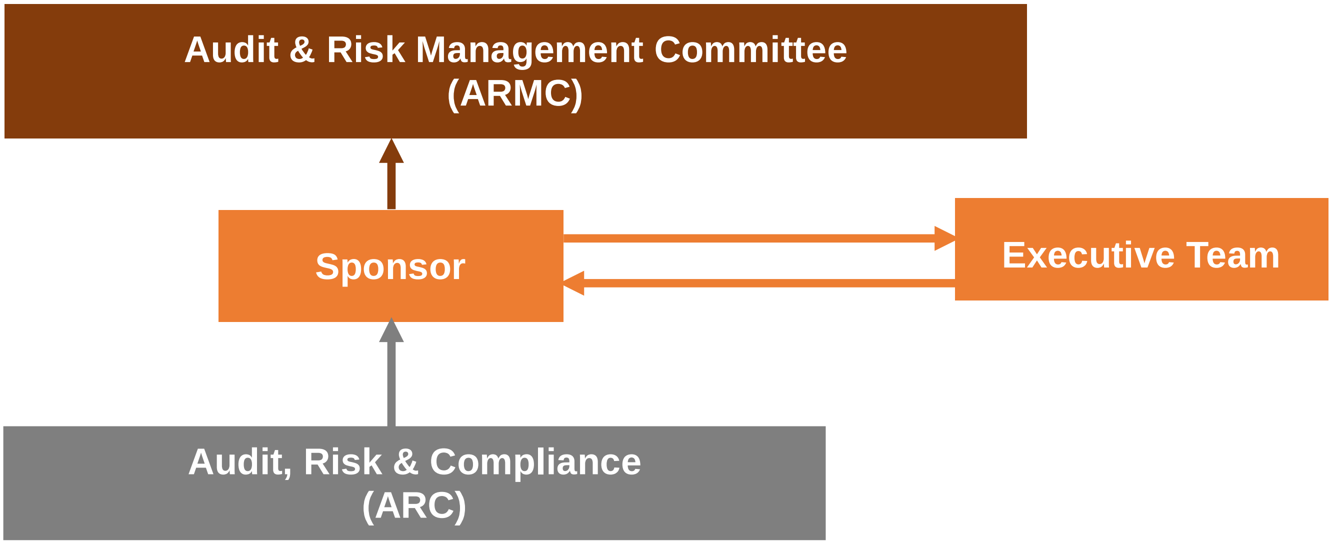
- **Risk management is everyone's responsibility:** The Board, all levels of management and individual employees are responsible for understanding the principal risks in their areas of responsibility and for making effective risk management decisions.

- **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 evolution:** 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:


Audit & Risk Management Committee (ARMC)
Sponsor
Executive Team
Audit, Risk & Compliance (ARC)

ROLES AND RESPONSIBILITIES

Audit & Risk Management Committee (ARMC)

The role of the ARMC 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.

ERM Sponsor

The ERM sponsor is the Deputy Chief Executive Officer (DCEO). The role of the ERM Sponsor is to:

- Set an appropriate tone from the top that supports the effective implementation of the ERM Framework.
- Provide oversight for the ERM Framework and activities.
- Monitor ERM Program efforts.
- Report ERM Program activities to the ARMC.
- Support accountability and action.
- Provide ongoing guidance and input to the ARC Department on the TTC's enterprise risks.

Executive Team

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

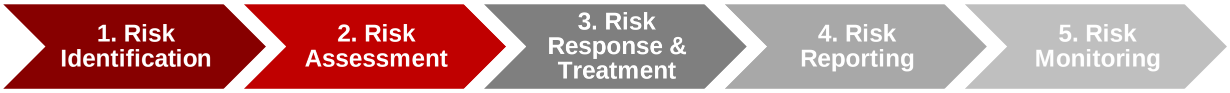
- Identify and manage risks across the TTC and adhere to the ERM Framework, process, procedures and Enterprise Risk Inventory.
- Be active sponsors and supporters of ERM Program activities and ensure adequate progress is being made on the achievement of desired control capabilities and timelines for mitigation.
- Manage and monitor risks within their areas, finalize mitigation plans as appropriate, and provide updates to ARMC 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 (ARC) Department

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 ARMC.
- 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.

The five major phases that constitute the ERM process are illustrated below:



1. Risk Identification

2. Risk Assessment

3. Risk Response & Treatment

4. Risk Reporting

5. Risk Monitoring

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 objectives of the TTC. 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 risk assessment process to evaluate inherent risk levels, assess current control capability against desired control capability, and determine the remaining risk after mitigation efforts.

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 and/or tolerance levels. 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

The **Risk on a Page Summary** Report provides a comprehensive and consistent method for risk reporting. Executive Risk Owners are responsible for presenting their risks, including the Risk on a Page Summary Report to the Executive Team for comments and feedback, and to regularly report progress until the desired control capability is in place and the desired risk level is reached. ARC will support Executive Risk Owners with presenting risk information to the ARMC, and Risk Owners are responsible for addressing questions by ARMC members on risk response / treatment, for example.

Executive Risk Owners must include the Risk on a Page Summary Report in any enterprise risk presentation provided to the Executive Team and/or ARMC. However, this can be used in conjunction with other presentation materials that may be used to enhance the audience's understanding of the risk and risk mitigation strategies.

Regular reporting of risk information is critical to support a robust ERM process and enable ARMC 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.

STEP 5: MONITORING

Risks and mitigations must be monitored on an on-going 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 Risk Analysis information as well as the Risk on a Page Summary Report. All risk actions are to be tracked to completion.

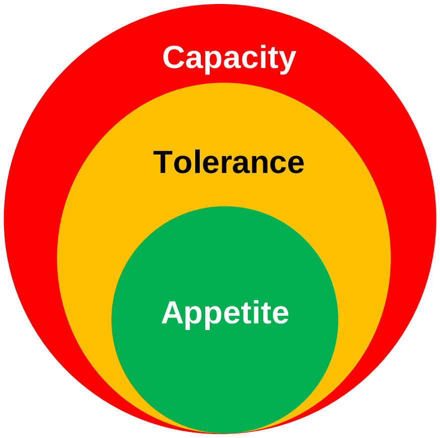
Risk information should be reviewed on a quarterly basis and actively updated as changes occur.

On an annual basis, the TTC ERM Framework and Enterprise Risk Inventory will be reviewed to ensure they reflect the corporate risk appetite, leading practice and are adapting to any changes in strategic objectives.

Risk Appetite and Tolerance

Risk appetite and tolerance need to be reviewed at regular intervals and approved by the ARMC. Factors such as new technology, or changes in business strategy may require the TTC to reassess its overall risk profile and reconfirm its risk appetite.

The TTC's Risk Capacity would always be greater as compared to tolerance and appetite, whereas, tolerance can be either equal to or greater than appetite.



Enterprise Risk Inventory

The Enterprise Risk Inventory is the TTC's risk register, which lists all enterprise risks and contains all of the risk-related documentation for each risk, including risk analysis and reports. The Enterprise Risk Inventory is updated whenever new risks are identified by the Executive or the level of a risk has changed. Incident investigation reports, historical risk assessments, leading industry practices, legal requirements/applicable legislation, and impacts of any interdependent risks may also be housed in the Enterprise Risk Inventory. Refer to the Enterprise Risk Inventory for the details of all key enterprise risks.

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 enable users to effectively apply the ERM Framework and procedures, and promote and reinforce an effective risk management culture at the TTC.

FRAMEWORK EXCEPTIONS

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

REFERENCES

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

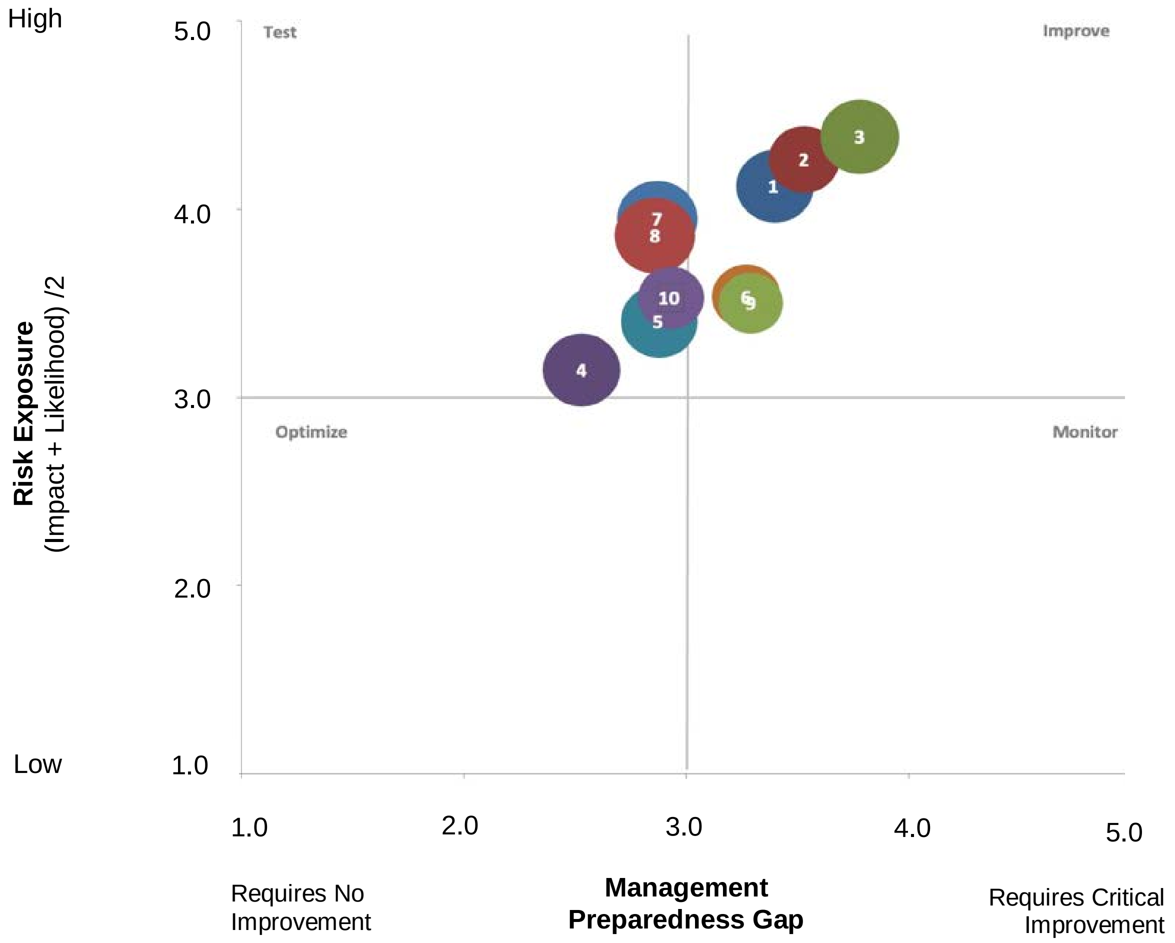
APPENDICES

DEFINITIONS

#	Key Term	Definition
1.	Enterprise	Any organization established to achieve a set of objectives.
2.	Risk	The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood[1].
3.	Control	Any action taken by management, the Board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.
4.	Likelihood	The probability or chance that an incident and its associated outcome will occur.
5.	Impact	The effect, outcome or consequence of a risk occurring.
6.	Inherent Risk	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.
7.	Residual Risk	The risk remaining after controls or mitigating actions have been put in place.
8.	Risk Capacity	The maximum level of risk to which the organization should/can be exposed.
9.	Risk Tolerance	The acceptable degree of variability or deviation from the expected level of risk that the organization is prepared to withstand in order to achieve its objectives.
10.	Risk Appetite	The amount and type of risk that the organization is willing to pursue or retain.
11.	Risk Score	The assessed level of inherent risk or residual risk for each risk, as determined by applying the guidelines set out in the Risk Assessment Procedure.

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

Leadership Top Risks Assessment – Consultant Workshop Results

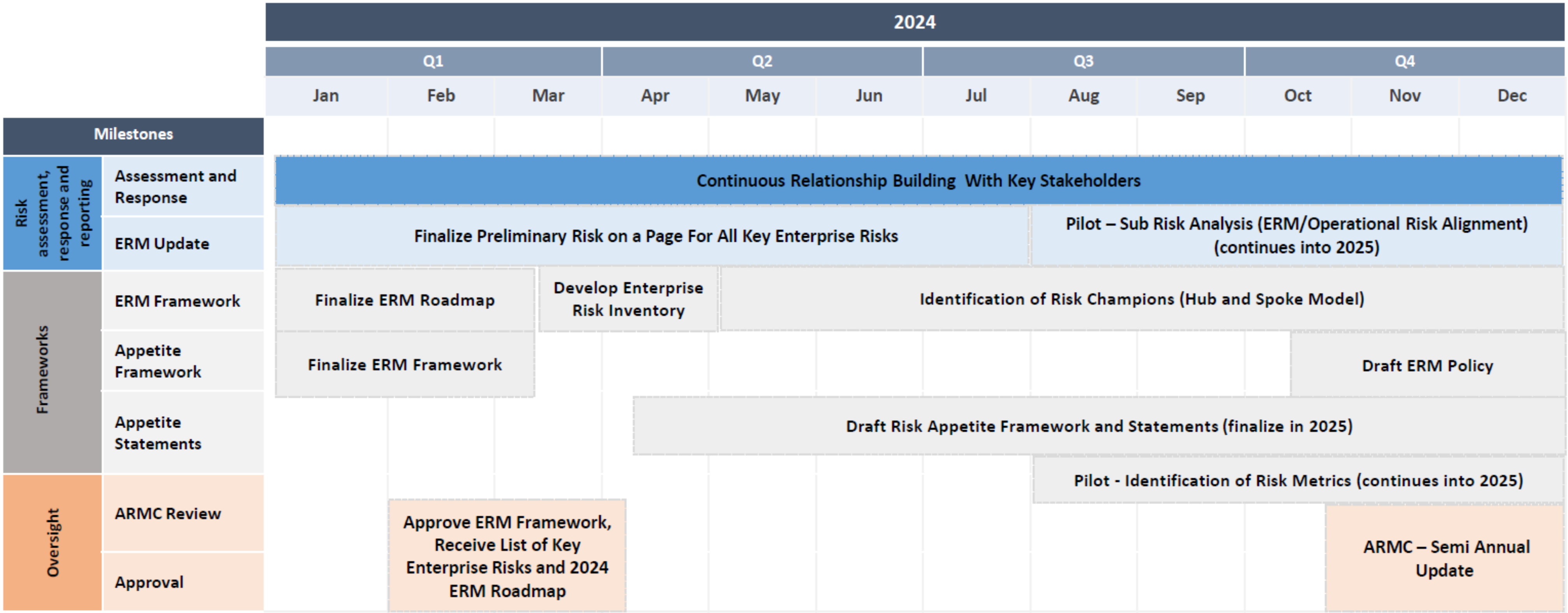


#	Risk Title	#	Risk Title
1	Financial sustainability	6	Governance and decision making
2	Capital funding requirements	7	Cybersecurity
3	Recruitment and retention	8	Disruption risk
4	Worker and customer safety	9	Strategy development and execution
5	Public safety and transit security	10	Third party vendor risk

Note: The tool used for scoring is a consultant tool however the results are management's conclusions during the workshop on Oct 26 2023.

Attachment 3

ARC 2024 ERM Roadmap



2024

Q1 Q2 Q3 Q4

Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec

Milestones

Risk assessment, response and reporting

Assessment and Response

Continuous Relationship Building With Key Stakeholders

ERM Update

Finalize Preliminary Risk on a Page For All Key Enterprise Risks

Pilot – Sub Risk Analysis (ERM/Operational Risk Alignment) (continues into 2025)

Frameworks

ERM Framework

Finalize ERM Roadmap

Develop Enterprise Risk Inventory

Identification of Risk Champions (Hub and Spoke Model)

Appetite Framework

Finalize ERM Framework

Draft ERM Policy

Appetite Statements

Draft Risk Appetite Framework and Statements (finalize in 2025)

Pilot - Identification of Risk Metrics (continues into 2025)

Oversight

ARMC Review

Approval

Approve ERM Framework, Receive List of Key Enterprise Risks and 2024 ERM Roadmap

ARMC – Semi Annual Update

This timeline is iterative and is subject to change based upon continuous discussions with leadership and key stakeholders.