For Action
with Confidential Attachment

Audit, Risk and Compliance – 2025 Enterprise Risk Management Update

Date: March 24, 2025
To: Audit & Risk Management Committee
From: Deputy Chief Executive Officer and Head of Audit, Risk and Compliance

Reason for Confidential Information

This report contains information related to the security of the property of the municipality or local board.

Summary

The Audit, Risk and Compliance Department (ARC) has been tasked with facilitating the maturity of the Enterprise Risk Management (ERM) Program at the TTC and provides this report to the Audit & Risk Management Committee (ARMC) to share information on the status of the ERM Program and to facilitate risk owners to report on their Key Enterprise Risks. In summary, this report provides an overview of the following items:

- **ERM Framework Review:** The ERM Framework was approved by the ARMC on March 19, 2024, and sets out roles and responsibilities, including the responsibility of the ARMC to annually review and approve any further changes to the ERM Framework. In response to consultant recommendations to align the ERM Program with industry best practice, ARC has added a Vision Statement to the ERM Framework to articulate the vision and guiding principles of the ERM Program. No further changes are being proposed except for this addition.

- **2025 ERM Roadmap:** This report provides the details of ARC's annual roadmap so that deliverables are highlighted early in the year. Systematically evaluating progress against annual goals ensures adequate progress and allows for refinement of actions, if necessary, to adapt to any changing priorities or emerging threats in the business environment.

- **ERM Multi-Year Maturity Roadmap**: A comprehensive roadmap outlining all planned activities necessary to develop and sustain a mature ERM Program is provided within this report. The Roadmap is based on consultant recommendations for implementation and is aligned with best practices. Based on these recommendations, the ERM Multi-Year Maturity Roadmap identifies short-, medium- and long-term actions across a five-year period that are required to bring the TTC's ERM Program to a desired level of maturity. It provides a holistic view of the program's planned ERM evolution.

- **Risk on a Page Summary Reports:** ARC has facilitated the completion of Risk on a Page Summary Reports for all 10 Key Enterprise Risks, which will allow for tracking and monitoring of progress on identified action plans to achieve desired control capability targets. In 2025, ARC will update all Risk on a Page Summary Reports to address feedback provided by Executive risk owners, including the addition of information regarding current control activities.

Key Enterprise Risks	
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

- **Risk on a Page Summary Report Presentation by Risk Owners:** ARC designed the Risk on a Page Summary Report template to assist management in providing a high-level overview of their risks, risk response strategies, and current state.

Recommendations

It is recommended that the Audit & Risk Management Committee:

1. Approve changes to the TTC's Enterprise Risk Management Framework.

2. Receive the confidential information and authorize that the information remain confidential in its entirety as it contains information about the security of the property of the TTC.

Financial Summary

The facilitation of the ERM Program by ARC has no funding implications beyond the costs of ARC that were included in the 2025 Operating Budget approved by the TTC Board on January 10, 2025.

The Executive Director – Finance has reviewed this report and agrees with the financial impact information.

Equity/Accessibility 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.

Decision History

On March 19, 2024, the ARMC approved the TTC's ERM Framework and received the list of top 10 Key Enterprise Risks and the 2024 ERM Roadmap.
Audit, Risk and Compliance – Enterprise Risk Management Update

On November 21, 2024, the ARMC received the ERM Year-End Update detailing the completion of 2024 deliverables as part of the ERM Multi-Year Maturity Roadmap.
Audit, Risk and Compliance – 2024 ERM Year-End Update

Issue Background

The TTC is continuing to build its ERM Program to strengthen risk management capabilities across the organization and provide the ARMC with more oversight over the management of key risks. Completion of the 2023 and 2024 Roadmaps established important foundational elements, including the ERM Framework, the establishment of the top 10 Key Enterprise Risks through an Executive Risk Workshop, and resourcing for an ERM function.

Building on this foundation, ARC will initiate the annual 2025 ERM Roadmap of deliverables details of which are provided herein. Additionally, ARC will facilitate risk owners to present the Risk on a Page Summary Report for Public Safety and Transit Security Risk, one of the top 10 Key Enterprise Risks. The presentation will provide the ARMC with details of the nature of the risk, proposed mitigation plans, and status.

Comments

ERM Framework

In response to consultant recommendations, ARC has drafted a Vision Statement. This addition articulates the overarching philosophy and purpose of ERM to establish risk-informed decision-making and to help the organization manage Key Enterprise Risks. The addition also confirms Leadership's commitment to supporting the program and associated activities. (See Attachment 1)

Future ERM Framework revisions may reflect the realignment of the TTC's Internal Governance Structure and ARC is working with the Corporate Initiatives Department to better understand the implications as it relates to the governance model for ERM. As part of the realignment, Leadership Tables have been established for each of the five strategic directions of the Corporate Plan. As ERM is a priority action under strategic direction 4, ERM progress updates have been assigned to Leadership Table 4:

Organization Transformation/Modernization. ARC will explore the need to capture Table 4 into the governance model for ERM and any changes will be incorporated into the next ERM Framework revision.

2025 ERM Roadmap

ARC is providing its 2025 ERM Roadmap and progress will be tracked throughout the year and reported on through the ERM Year-End Update. In 2025, ARC will continue to make significant strides in maturing ERM at the TTC. ARC will:

- Continue to consult on ways to align operational and enterprise risk, including a process that escalates high and very high operational risks to ERM for review.
- Working with IT Services and other stakeholders to review system tool requirements to support integration of Audit, Risk and Compliance information and reporting, and link risk registers across the organization.
- Consult with the Executive Team on a Risk Appetite Framework and establish Risk Appetite Statements.
- Enhance Risk on a Page Reports for all 10 Key Enterprise Risks based on lessons learned/feedback.
- Commence assessment of significant sub risks to determine the impact on Key Enterprise Risks.
- Determine ERM Program KPIs.

(See Attachment 2)

ERM Multi-Year Maturity Roadmap

The ERM Multi-Year Maturity Roadmap, which was designed based on consultant recommendations, facilitates the development of a comprehensive and effective risk management program that is aligned with industry best practices. The document establishes a solid foundation for the program by encompassing initial elements, such as resourcing, training and workshops, medium-term elements, such as the ERM Framework, policy and procedure documents and longer-term actions that support achieving the desired state of maturity. These longer-term actions include risk appetite statements linked to risk metrics, continuous monitoring and reporting and a system tool that links enterprise to operational risk management. ARC is providing the ARMC with this multi-year holistic view to better facilitate understanding of the components necessary for effectively building an ERM Program that fully promotes a risk aware culture and risk-informed decision-making. (See Attachment 3)

Risk Appetite Framework Development

The Enterprise Risk Appetite Framework is a key element of the ERM Program designed to support consistent management and monitoring of risk within risk appetite tolerances. The first step is to establish qualitative Risk Appetite Statements that define the level of risk the TTC is willing to take. Next, quantitative risk metrics will be defined for each risk so that trends in risk level can be tracked and monitored. This activity supports the fifth step of the risk management process: identify, assess, respond, report, and ***monitor*** risk.

ARC has drafted qualitative Risk Appetite Statements for all 10 Key Enterprise Risks. The next step is for ARC to facilitate respective risk owners to review and formally attest to these statements. Once finalized, ARC can then commence work to establish the associated quantitative metrics that will be used to monitor risk levels to ensure risks are being managed within the established tolerance. Risk Appetite discussions will be the focus of Executive consultations in 2025 followed by confirmation of qualitative risk metrics in 2026.

Conclusion

This report reflects the TTC's commitment to embedding robust risk management practices and fostering a proactive risk culture throughout the organization. The enclosed materials aim to provide the ARMC with the necessary information to fulfill its oversight role for ensuring an ongoing process is in place for managing Key Enterprise Risks through the TTC's ERM Program and associated risk reporting.

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 – 2025 ERM Roadmap
Attachment 3 – ERM Multi-Year Maturity Roadmap
Attachment 4 – Confidential Information

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 & 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 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.

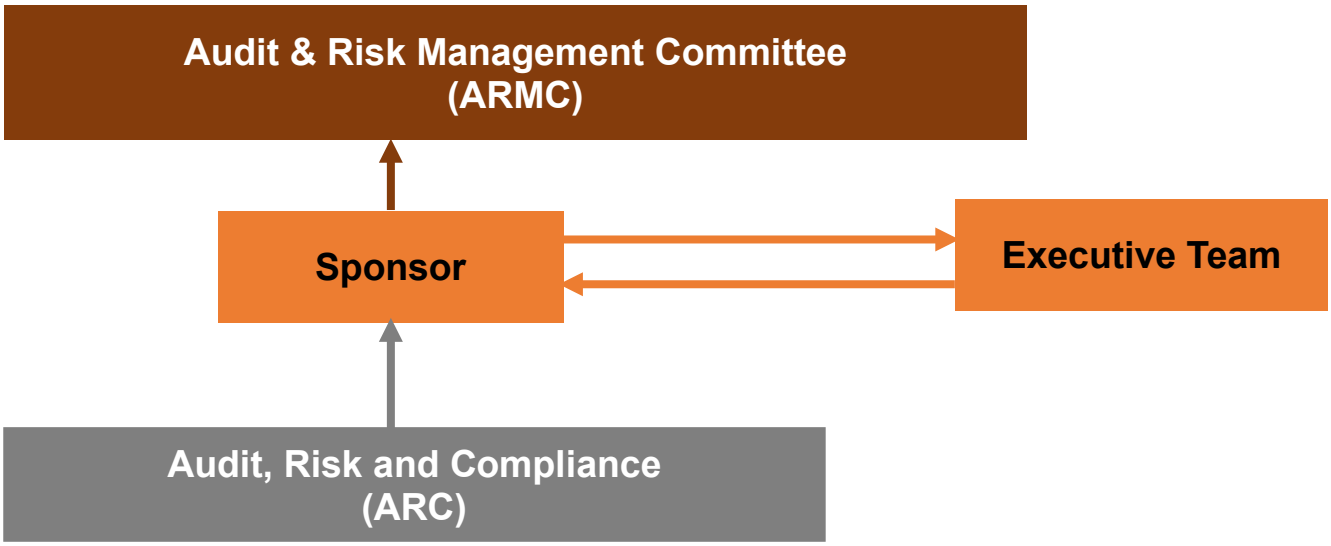
- **Significant risks are identified and managed through an integrated approach:** A comprehensive, disciplined and consistent approach to risk management will be ongoing and integrated with other risk management areas.

- **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:



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 the 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 the 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:

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 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 the 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 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 Risk Analysis information as well as the Risk on a Page Summary Report. All risk actions are to be tracked to completion.

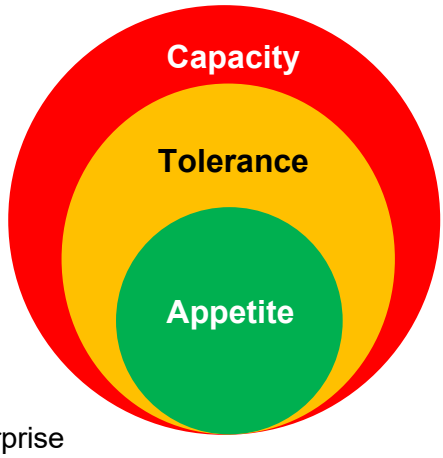
Risk information should be reviewed on a quarterly basis and actively updated as changes occur.

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 that 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 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.

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

APPROVALS AND REVISION HISTORY

The ERM Framework was last reviewed and approved by the ARMC on March 24, 2025.

Version	Date	Author(s)	Revision Notes	Review	Approval
V1	March 19, 2024	Director, ARC	ERM Framework V1	Head – ARC	ARMC
V2	March 24, 2025	Director, ARC	Annual Review and Inclusion of Vision	Head – ARC	ARMC

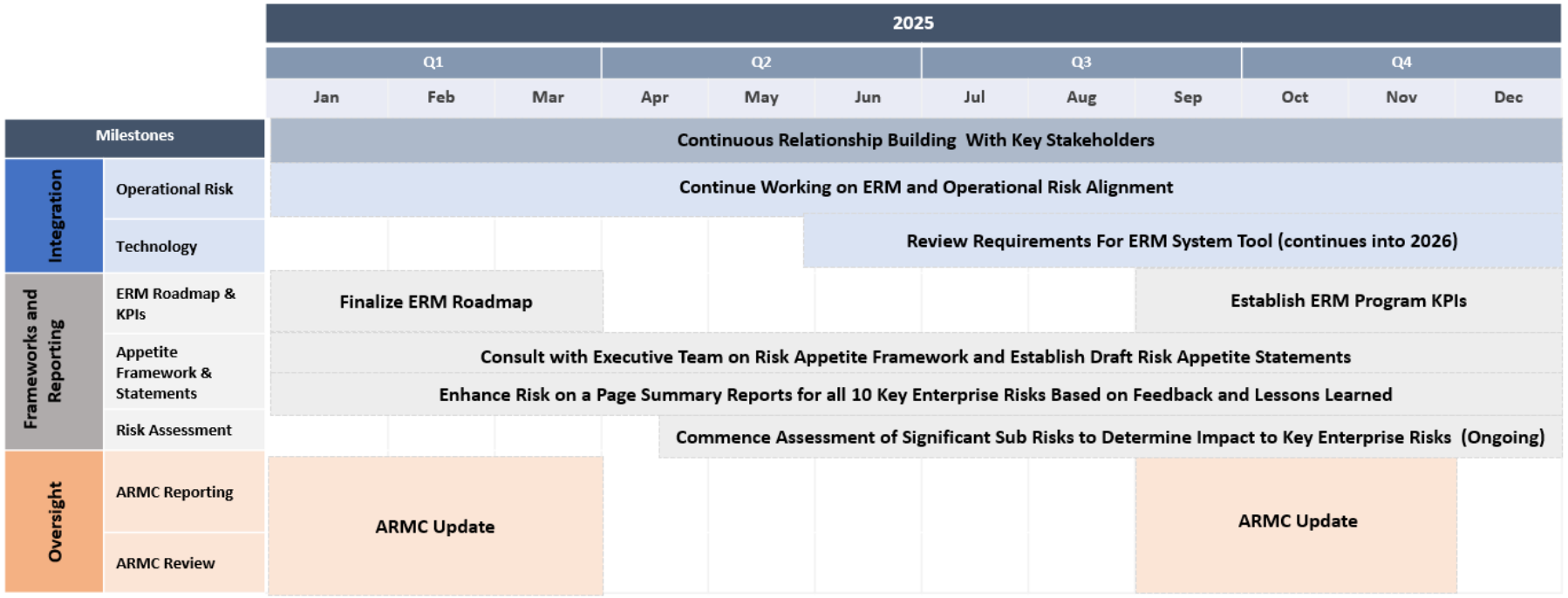
APPENDICES

DEFINITIONS

#	Key Terms	Definitions
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 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.	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	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.
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, is determined by applying the guidelines set out in the Risk Assessment Procedure.

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

ARC 2025 ERM Roadmap



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

ERM Maturity Roadmap

Legend: Short Term | Mid- Term | Long Term

		Risk Governance and Oversight	Risk Vision and Appetite	Strategic and Enterprise Risk Assessment	Operational Risk Processes	Coordinated Risk Management	Enabling Technology
Level 1: Basic Short Term 1-2 Years	2023	Draft ERM Framework	Consultant Recommendations	Risk Identification Workshop			
		Executive Sponsor		Draft Risk Assessment Tools			
		ARMC Training		Resourcing			
				Initial Assessment			
	2024	ERM Framework Approval	Draft ERM Policy	Mapping of Key Enterprise Risks to the Corporate Plan	Commence Operational Risk Pilots Facilitation		
		Risk Inventory	Draft Risk Appetite Framework and Statements	Finalize Preliminary Risk on a Page Reports			
Level 2: Developing Medium Term 2-3 Years	2025	Annual ERM Framework Refresh	Consult Executive to Review and Finalize Risk Appetite Statements	Enhance Risk on a Page Reports for all 10 Key Enterprise Risks based on lessons learned and feedback	Commence assessments of significant sub-risks to determine impact on 10 key risks (Ongoing)	Continue working on ERM and Operational risk alignment	Review requirements for ERM system tool
				Establish ERM Program KPIs			
	2026	Annual ERM Framework Refresh	Consult Executive to Establish Risk Tolerance Limits to Support Risk Appetite Statements - KRIs	Biennial Risk Identification Refresh	Continue assessments of significant sub-risks to determine impact on 10 key risks (Ongoing)	Continue working on ERM and operational risk alignment	Procure ERM system solution
		Risk On A Page Reporting			Consult on process for escalating significant Operational Risks to ERM		
Level 3: Evolved Long Term 4-5 Years	2027	Annual ERM Framework Refresh	Risk Appetite Framework Approval		Continue assessments of significant sub-risks to determine impact on 10 key risks (Ongoing)		Implement ERM system solution
		Draft Operational Risk Management Framework				Education and Training	
		Risk on a Page Reporting & Updates					
	2028	Annual ERM Framework and Risk Appetite Refresh	Monitoring and Reporting KRIs		Continue assessments of significant sub-risks to determine impact on 10 key risks (Ongoing)	Education & Integration	Live GRC and other necessary tools
		Operational Risk Management Framework Approval				ERM Program Review and Continuous Improvement	
		Risk on a Page Reporting & Updates					