METROLINX

MEMORANDUM

To: Metrolinx Board of Directors

From: Robert Siddall
Chief Financial Officer

Date: September 14, 2017

Re: **ERM Policy and Framework**

Executive Summary

Attached are the draft Enterprise Risk Management (ERM) Policy and Framework which were reviewed by the Audit, Finance and Risk Management Committee on September 13, 2017.

The existing ERM Policy was approved in 2010. Over the last seven years, the scale and complexity of Metrolinx's operations and projects has increased significantly and best practice in ERM would include ongoing review of our policy and framework. To obtain an independent opinion on the maturity of the ERM program, Pricewaterhouse Coopers (PwC) was invited to conduct a health check, the results of which were reported to AFaRM in February 2017. Based on PwC's assessment and AFaRM's recommendations, the ERM team developed a work plan and began the process of reviewing and updating key components of the program.

The draft ERM Policy and Framework have been developed in consultation with various business units across the organization. The following reflects some of the key changes which have been made:

- responsibilities have been more clearly articulated;
- the frequency of risk review by management has been increased from quarterly to monthly;
- the framework expressly requires that risk management be embedded into decision making, and be aligned with strategic objectives and the annual strategic planning process.

The ERM work plan includes engaging the Board on risk identification and the development of a formal risk training program will begin in fall 2017 and risk appetite and risk scoring criteria will be brought before the Board in 2018.

Recommendation

THAT, the Board approve the following resolution:
RESOLVED:

THAT the Enterprise Risk Management Policy and Framework be approved.

Background

Risk management and oversight of risks at the strategic, corporate and the business unit or project level is integral to the successful achievement of Metrolinx's strategy and operations. An effective enterprise risk management program provides the basis for risk-informed decision-making and risk awareness throughout the organization. The foundation of a good ERM program is the development, implementation and ongoing review of a best practice based ERM policy and framework.

The existing ERM Policy was approved in 2010. Over the last seven years, the scale and complexity of Metrolinx's operations and projects has increased significantly and best practice in ERM would include ongoing review of our policy and framework. To obtain an independent opinion on the maturity of the ERM program, Pricewaterhouse Coopers (PwC) was invited to conduct a health check, the results of which were reported to AFaRM in February 2017. Based on PwC's assessment and AFaRM's recommendations, the ERM team developed a work plan and began the process of reviewing and updating key components of the program.

Policy and Framework

Essential elements of and effective ERM program include:

- enterprise wide approach to risk
- links to strategy, business resiliency and sustainability
- clearly defined processes for risk identification, assessment, response, monitoring and reporting
- set risk appetite and tolerance
- clear responsibility, accountability and ownership
- regular, standardised quantitative and/or qualitative reporting
- standardised language

The proposed ERM policy and framework are based in part on the revised COSO Enterprise Risk Management framework[1] as well as ISO 3100:09[2] Risk Management standards. The policy and framework also take into consideration Metrolinx's current business environment and level of risk maturity. The vision for ERM at Metrolinx is that: "Enterprise risk management (ERM) enhances the governance and management activities of Metrolinx, supporting the culture, and establishing risk-informed decision-making throughout the organization."(p.1)

[1] COSO - The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of (the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, the IMA - Association of Accountants and Financial Professionals in Business, and the Institute of Internal Auditors)and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.

[2] ISO – The International Organization for Standardization which develops international standards. ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.

The policy provides direction and overview in regards to ERM. The framework outlines:

- the link between strategy and risk (p.1)
- the risk process (p. 2-3)
- responsibility for oversight of risks (Table1)
- ownership of risks and action plans (Table1)
- the requirements for regular (monthly or quarterly) risk assessment and review of strategic, financial, operational, safety and project risk at appropriate levels (Business Unit/Project, MAFaRM, SMT, AFaRM, Board)
- definitions for risk management (p. 6-7)

Respectfully submitted,

Robert Siddall
Chief Financial Officer

Attachments:

1. Draft Metrolinx Enterprise Risk Management Policy
2. Draft Metrolinx Enterprise Risk Management Framework

ENTERPRISE RISK MANAGEMENT POLICY

ERM Vision

Enterprise risk management (ERM) enhances the governance and management activities of Metrolinx, supporting the culture, and establishing risk-informed decision-making throughout the organization.

Policy Statement

Metrolinx will adopt best practices in the identification, assessment, response, monitoring and reporting of risks that affect our ability to achieve our objectives and strategy. Risk management will be embedded across the organization and become an integral part of decision making from strategic planning to daily operations.

This policy is a statement of commitment by the Board of Directors and management of Metrolinx to ensure the introduction, adoption and implementation of an effective risk management system throughout the corporation.

ERM activities form an integral part of Metrolinx's objective setting process. It supports and improves the decision-making, planning and prioritization processes to ensure appropriate action is undertaken to continually address risks facing the corporation, and align Metrolinx's resources to deliver our commitment of service to our customers. ERM is an ongoing, proactive and dynamic process to identify, assess, respond to, monitor and report risks that may impact objectives.

This ERM Policy statement serves as an umbrella over the Metrolinx enterprise risk management framework (the framework), and all other risk management practices and frameworks at Metrolinx.

The objectives of enterprise risk management are to:

- Support the achievement of Metrolinx's mission, vision and strategic priorities in line with its core values;
- Integrate risk management in the culture and strategic decision-making across the organization;
- Anticipate and respond to changing social, environmental and legislative conditions;
- Adopt best practice in the management of risk;
- Align risks with Metrolinx's risk appetite and tolerance;

- Establish structured processes for identifying, assessing, responding to, monitoring and reporting on risk;
- Enable Metrolinx to fulfil its commitment to its customers and community to engage them, treat them with respect, consideration, seek their input, keep them informed, ensure their safety, invest public funds responsibly and build and operate transit that connects communities;
- Fulfill Metrolinx's social responsibilities, protect its reputation and preserve key relationships.

These objectives will be achieved by:

- Setting corporate strategy in line with Metrolinx's risk appetite and tolerance;
- Establishing a risk management organizational structure across all levels of Metrolinx;
- Adopting a framework and processes to guide enterprise risk management in line with best practice;
- Creating a system of accountability to ensure that risks are managed systematically and proactively;
- Establishing systems of reporting to ensure the Board and senior management is regularly apprised of risk management activities;
- Maintaining effective communication and involvement of all staff;
- Providing regular training in risk management.

Responsibilities

In order to ensure the achievement of Metrolinx's risk management objectives, involvement is required at all levels of the organization.

The framework lists detailed responsibilities of all groups involved in the risk management process. The key responsibilities of each group are as follows:

The Board of Directors

The Board of Directors oversee ERM activities, provide support and direction by:

- Reviewing and approving the ERM policy and framework every two years.
- Annually reviewing and approving corporate risk appetite and tolerance.

- Delegating to the Audit, Finance and Risk Management Committee, the responsibility for implementing the enterprise risk management process and framework, including identification, assessment, response, monitoring and reporting of enterprise risks, and ensuring that appropriate measures are in place to manage such risks.

- Receiving and reviewing:

    - Annually all enterprise risks in context of Metrolinx's annual strategy review.

    - A quarterly update of enterprise risks, considering them against the set risk appetite and tolerance and also reviewing management's response to them.

    - Any additional risk reporting that the Audit, Finance and Risk Management Committee brings to the attention of the Board.

Audit, Finance and Risk Management Committee

Oversees the ERM process by ensuring that it is effectively implemented at all levels of the organization, and regularly reviews enterprise risks. Reviews the policy, framework, risk appetite and tolerance and recommends them for Board approval.

For detailed responsibilities see Audit, Finance and Risk Management Committee terms of reference.

Other Committees of the Board

Regularly review ERM activities and enterprise risks as they relate to the function of their committees.

Senior Management Team

Implements the enterprise risk management framework and sets the risk culture. Reviews enterprise risks, risk appetite and tolerance and recommends them to the Audit, Finance and Risk Management Committee.

Management, Audit, Finance and Risk Management Committee

Provides oversight to the enterprise risk management process, regularly reviews enterprise risks and reviews and endorses risk appetite and tolerance.

Enterprise Risk Management Group

The Chief Financial Officer has an obligation to report to the Audit, Finance and Risk Management Committee, and the Board the key risks facing the corporation.

The ERM team executes, supports and coordinates activities related to the ERM process, and educates on risk management.

Internal Audit

Provides independent assurance on the state of risk management, and considers high and very high risks for the annual internal audit plan.

Business Unit/ Project Management

Business units/ project management are accountable for all risks facing the business unit/ project and for managing them in line with the framework, including maintaining a risk register, ensuring risks are within the set appetite and tolerance and escalating risks as appropriate.

Risk Owners

Accept responsibility for managing specific risks, monitoring and reporting on progress and effectiveness of the risk response.

Risk Managers

Accept responsibility through delegation from the risk owner for managing specific risks, monitoring and reporting on progress and effectiveness of the risk response.

Action Owners

Develop and execute action plans within the risk response plan, monitoring and reporting on progress of action.

Risk Champions

Maintain and update the risk register, and coordinate with ERM Group.

Frontline Staff

Report all actual or potential incidents and issues which present risks to the business unit or corporate objectives and strategy, to relevant business unit managers.

Metrolinx

An Agency of the Government of Ontario

Enterprise Risk Management Framework

September, 2017

Contents

1. **Overview**
1.1 Enterprise Risk Management Vision
1.2 Risk and Enterprise Risk Management

2. The Enterprise Risk Management Process
2.1 Key Features
2.2 Five Step Risk Management Process

3. Responsibilities

4. Definitions

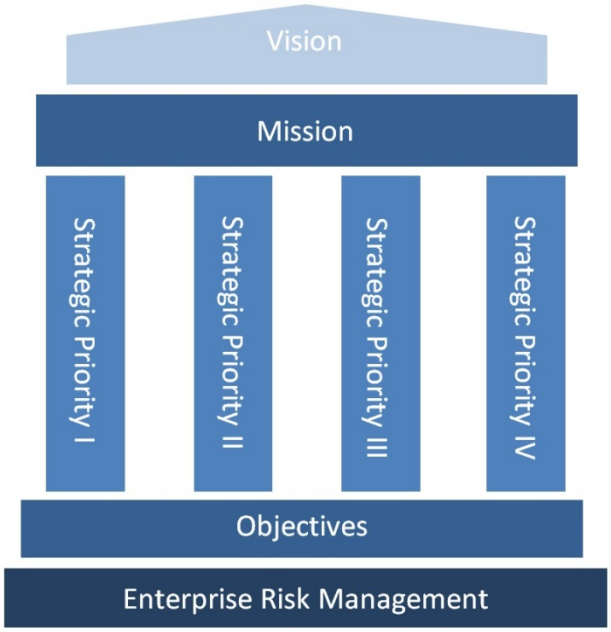
1. Overview

1.1 Enterprise Risk Management Vision

Enterprise risk management (ERM) enhances the governance and management activities of Metrolinx, supporting the culture, and establishing risk-informed decision-making throughout the organization.

1.2 Risk and Enterprise Risk Management

Risk is the possibility that events will occur and either positively or negatively affect the achievement of strategic priorities and business objectives. ERM is a systematic and proactive process to oversee, manage and report such risks across all parts of the organization, within the risk appetite and tolerance thresholds set by the organization, ensuring the most efficient response to risk to which the organization is exposed.



The risk management process and the oversight of key risks informs our strategic objectives and priorities. To achieve our vision and the fulfill our commitments, we define our strategy and implement ERM making it an integral part of strategic decision making, objective setting and operations, across the organization.

2. The Enterprise Risk Management Process

2.1 Key features

ERM is an ongoing and continuously improving process which is regularly reviewed to improve, adapt and respond to changing circumstances. Risk management is key across all of Metrolinx and is supported by continuous risk awareness training at all levels of the organization.

2.2 Five Step Risk Management Process

i. Risk Identification

The purpose of risk identification is to develop a comprehensive list of events that may affect the achievement of objectives. This process may be conducted by way of discussions, workshops, brainstorming and looking at the past. All risks identified will fall into one the following categories:

- *Project risks*
- *Operational risks*
- *Financial risks*
- *Strategic risks*
- *Safety risks*

In addition to identifying known risks, a deliberate and concerted effort must be made to identify emerging risks.

ii. Risk Assessment

Risk assessment is the process of measuring the level of exposure that each risk presents to the objectives of Metrolinx, the business unit or project by quantifying it`s likelihood of occurrence and potential impact by applying the risk criteria.

Risk at the present time is known as current risk and is quantified after taking into account all existing controls, and other mitigation techniques that are already in place.

iii. Risk Response

The current risk level is unacceptable when it is outside of our risk appetite and tolerance, or is identified as medium, high or very high. For all such risks, a risk response plan must be developed with the purpose of bringing the risk to an acceptable level or the target risk level.

The risk response plan must consist of one or more actions, with action owners, which in combination will close the gap between the current risk level and the target risk level.

iv. Risk Monitoring

Risks and their corresponding response plans must be monitored on an ongoing basis. The key purpose of monitoring is to:

- determine the effectiveness of the risk response plan, and if necessary revise it;
- obtain new information that may affect risk assessment;
- analyze events, trends, successes and failures;
- observe changes in the internal and external environment, and their impacts on risk assessment, and response plans.

v. Risk Reporting

- Key business unit/ project management risks are reviewed and updated in the risk register every quarter, with significant changes to risks and identification of new risks being updated every month.

- Enterprise risks are reported to the Senior Management Team and the Management, Audit Finance and Risk Management Committee every quarter, with significant changes to risks and identification of new risks being reported every month.

- Key enterprise risks are reported to the all appropriate Board Committees and the Board every quarter.

For further details on risk reporting see Section 3: Responsibilities

3. Responsibilities – Table 1

Responsibility for ERM lies across the organization, specific responsibilities are as follows:

	Policy and Framework	Risk Appetite and Tolerance	Risk Reporting	ERM Process
The Board	Review and approve every two years	Annual review and approval	Quarterly review	Delegation to AFaRM Align strategy with key risks annually
Audit, Finance and Risk Management Committee	Review and recommend to Board every two years	Annual review and recommendation to Board	Quarterly review	Ongoing responsibility for oversight
AFaRM Vice Chair	Review and recommend to AFaRM every two years	Annual review and recommendation to AFaRM	Regular review and follow up	Monitor progress
Other Board Committees	Awareness of policy and framework	Ensure risks are within appetite and tolerance	Quarterly review of functional risks Report concerns to AFaRM	Review and monitor as related to committee function
Senior Management Team (SMT)	Review and recommend to AFaRM every 2 years	Annual review and recommendation to AFaRM	Quarterly review Monthly review of significant changes	Ongoing responsibility for risks and action plans Align strategy with key risks annually
Management, Audit, Finance and Risk Management Committee	Review and recommend to SMT every 2 years	Annual review and endorsement	Quarterly review Monthly review of significant changes	Ongoing responsibility for review and discussion
ERM Group	Develop and maintain	Develop and maintain and disseminate	Oversee risk reporting process	Monitor, coordinate, and facilitate ERM process Training and awareness
Internal Audit	Independent assurance	Independent assurance	Assessment and audit	Independent assurance
Business Units/ Project Management	Awareness of policy and framework	Awareness of appetite and tolerance	Monthly update of significant changes, Quarterly update of risk registers	Adherance Coordination with ERM group

Risk Owners Risk Managers/ Champions	Awareness of policy and framework	Awareness of appetite and tolerance	Monthly update of significant changes, Quarterly update of risk registers	Acceptance of responsibility for risks and action plans
Frontline Staff	Report all actual and potential incidents to business unit managers.			

Definitions

Action Owner – The person responsible for execution of an action in the risk response plan.

Culture – The attitudes, behaviors, and understanding about risk that influence the decisions of management and personnel.

Current Risk Level – Magnitude of risk at the present point in time, after accounting for the effectiveness of all existing controls, expressed in terms of likelihood and impact, as defined by risk scoring criteria.

Emerging Risk – Risk that is known to exist but has not occurred sufficiently so that it's underlying causes, likelihood of occurrence and impacts may be known or understood with a reasonable level of confidence.

Enterprise Risk – Risk that impacts the ability of the organization to achieve its strategy and objectives.

Enterprise Risk Management – The culture, capabilities, and practices, integrated with strategy-setting and its execution that organizations rely on to manage risk and realize objectives.

Impact – Outcome or result of a risk, as defined by risk scoring criteria

Level of Risk – Magnitude of a risk expressed in terms of likelihood and impact, as defined by risk scoring criteria.

Likelihood – The chance of something happening, as defined by risk scoring criteria.

Project – For the purpose of this framework, projects includes those over $50 million or those that effect the organization significantly, e.g.: Enterprise Asset Management, Enterprise Documents and Records Management System, Enterprise Resource Planning.

Risk – The possibility that events will occur and affect the achievement of strategy and business objectives.

Risk Appetite – The amount and type of risk an organization is willing to accept in pursuit of its strategic priorities and objectives.

Risk Assessment – The process of determining the likelihood of occurrence and potential impact of a risk.

Risk Categories:

Project risks – Risks relating to a project being completed on time and on budget.

Operational risks – Risks relating to on-going operations.

Financial risks – Risks relating to and/ or impacting funding of projects and operations, liquidity, financial reporting and movements in price of products and services, interest rates, currencies and commodities.

Strategic risks – Systemic risks that are external to Metrolinx and outside its control, including economic, demographic and political risks.

Safety risks – Risks to the safety of Metrolinx's customers, staff, contractors and communities it operates and builds in.

Risk Champion – The point of contact within a business unit/ project who coordinates the risk management process, working with team members to ensure the identification, assessment, response, monitoring and reporting of risk; working with the ERM team to validate updates to the risk register.

Risk Criteria – Terms of reference against which a risk is scored and analysed.

Risk Level – See Level of Risk

Risk Identification – The process of finding, recognizing and describing risks.

Risk Management – Coordinated activities to direct and control an organization with regard to risk.

Risk Manager – The person, through delegation from the risk owner, with the responsibility and authority to manage a risk.

Risk Monitoring – Continual review, supervision, and critical observation in order to determine suitability, adequacy and effectiveness of risk assessment and risk response.

Risk Owner – The most senior person accountable for the risk.

Risk Reporting – Continual and regular formal process to provide, share or obtain information regarding the management of risk.

Risk Response – Process to modify risk. Risk response can involve:

- *Risk prevention* – to reduce the likelihood of occurrence,
- *Risk reduction* – to reduce the potential impact of an occurrence,
- *Risk avoidance* – to cease the activity giving rise to the risk,

- *Risk transfer* – to pass on liability of the risk to a third party, e.g. insurance
- *Risk retention* – to consciously decide to retain a risk and,
- *Risk exploitation* – to actively assume risk to exploit an opportunity.

Tolerance – or "risk tolerance". The amount of variation from a specific objective that is acceptable, as defined by risk appetite.

Target Risk Level – Magnitude of risk at a specified future point in time, expressed in terms of likelihood and impact, as defined by risk scoring criteria.