REPORT FOR ACTION

Status Update on the City-wide Risk Governance Model

Date: November 14, 2023
To: Audit Committee
From: Chief Technology Officer, Chief Information Security Officer, Executive Director, Toronto Emergency Management and Acting Director, Internal Audit

SUMMARY

This report outlines the governance model, processes, and activities that will contribute to overall Enterprise Risk Management within the City. Enterprise Risk Management (ERM) is a structured, consistent, and continuous process that supports the achievement of the organization's objectives by identifying, assessing, responding to, and reporting on the full spectrum of risk, holistically across the organization. It also manages the combined impact of those risks as an interrelated risk portfolio.

The report provides an overview of the proposed City-wide Risk Governance Model. The governance model outlines roles and responsibilities within the ERM process with respect to oversight of risks throughout the organization, including risks pertaining to business continuity, cyber major incident, and technology disaster recovery.

While divisions across the City including Technology Services, the Office of the Chief Information Security Officer and Toronto Emergency Management have employed their own processes to manage and govern their respective risks, ERM takes a holistic approach to risk management looking at risks from a City-wide perspective.

RECOMMENDATIONS

The Chief Technology Officer, Chief Information Security Officer, the Executive Director, Toronto Emergency Management, and the Acting Director, Internal Audit recommends that:

1. Audit Committee receive this report for information.

FINANCIAL IMPACT

There are no financial impacts on the current year’s budget arising from this report. However, the implementation of the City-wide Risk Governance model referred to in this report may result in financial implications which will be included in future years’ budget submissions of the relevant divisions for consideration and approval.

The Chief Financial Officer and Treasurer has reviewed this report and agrees with the financial implications as identified in the Financial Impact section.

DECISION HISTORY

On July 19, 2022, City Council requested that the City Manager, in co-ordination with the Chief Technology Officer, the Chief Information Security Officer, the Executive Director, Toronto Emergency Management and the Director, Internal Audit, to report to the Audit Committee in the third quarter of 2023 with a City-wide Risk Governance Model addressing risks related to business continuity, cyber major incident and technology disaster recovery.
Agenda Item History - 2022.AU13.9 (toronto.ca)

On November 2, 2021, Audit Committee requested the City Manager to report to the Audit Committee with information from each City of Toronto division, agency and corporation on their Information Technology Disaster Recovery Plan should the City's systems, technology, communications, or backups be made unavailable. In addition, the Chief Technology Officer was requested to report to the Audit Committee with an update on the status of City of Toronto's Corporate Technology Services Disaster Recovery Plan, including implementation, testing and a full project plan for any outstanding work.
Agenda Item History - 2021.AU10.8 (toronto.ca)

On May 26, 2008, City Council adopted audit report AU 7.3 - Disaster Recovery Panning for City Computer Facilities. The report provided a snapshot of what the City Status update of IT Disaster Recovery Plan has accomplished and what work remains to be completed in preparing contingency plans in the event of a disaster disabling City technology infrastructure.

COMMENTS

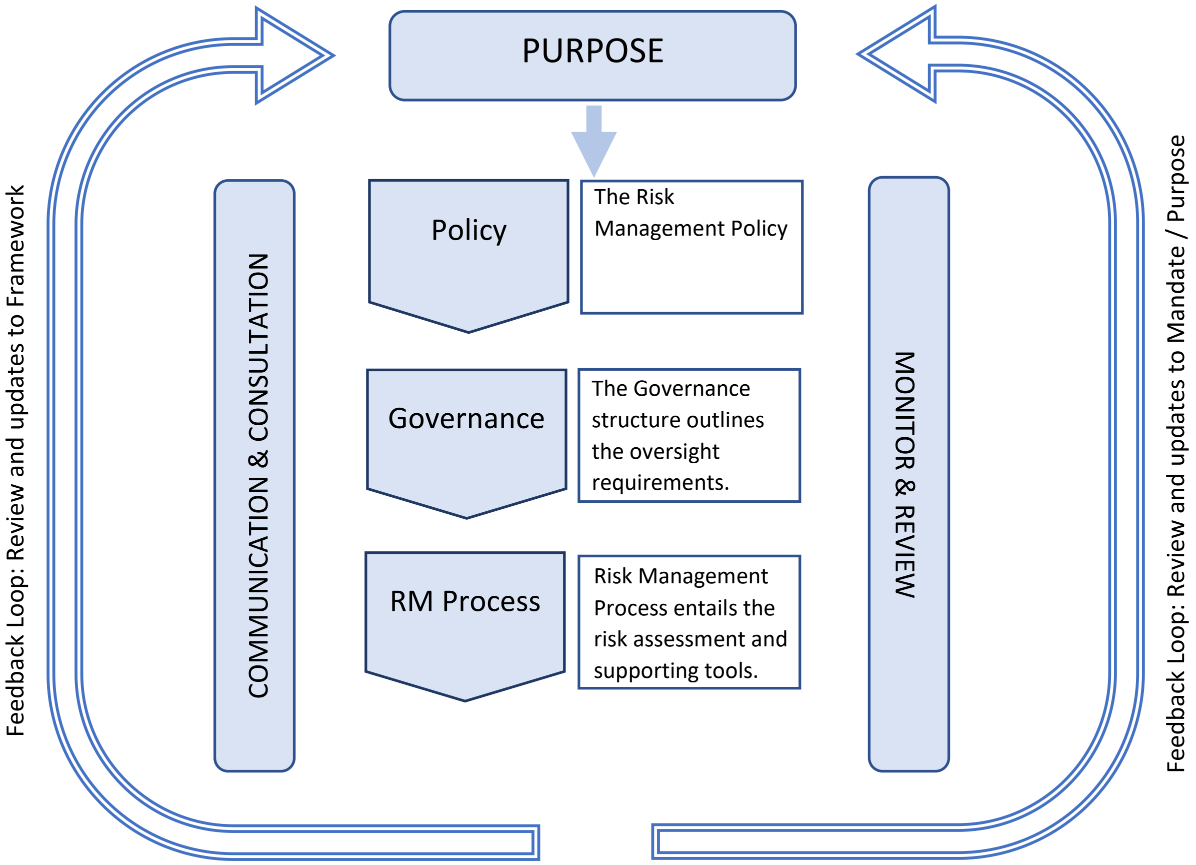
1. Enterprise Risk Management Overview

Enterprise Risk Management (ERM) is a holistic, disciplined approach to identifying, addressing, and managing an organization's risks. ERM looks at risk management strategically from an enterprise-wide perspective and advances the business objectives of the City. The aim is to embed this approach in a consistent and structured manner throughout the City’s business operations, and decision-making processes.

The purpose of ERM is to enable the City to:

- Create a more risk focused culture;
- Enhance decision-making leading to better management and resource optimization;
- Protect the City by managing risks effectively;
- Integrate ‘risk management’ into daily activities and decision-making
- Allow the City to adapt and respond to changes and disruptions, and enhance resilience

The **ERM Framework**, presented below, is a tool to guide the risk management process in a consistent manner, and includes the following components:


PURPOSE
Feedback Loop: Review and updates to Framework
COMMUNICATION & CONSULTATION
Policy
The Risk Management Policy
Governance
The Governance structure outlines the oversight requirements.
RM Process
Risk Management Process entails the risk assessment and supporting tools.
MONITOR & REVIEW
Feedback Loop: Review and updates to Mandate / Purpose

2. Risk Governance Model

The Risk Governance model provides an overview of roles and responsibilities to ensure risks are identified, communicated and managed effectively. It presents guiding principles for how accountabilities are distributed throughout the City to ensure appropriate engagement and governance of risk management activities.

	RISK MANAGEMENT RESPONSIBILITIES
CITY MANAGER	• Overall risk management accountability • Report significant risks to Council
SENIOR LEADERSHIP TEAM	• Incorporate risk management into strategic planning • Review risks holistically across the City • Assign Risk Leads
DIVISION HEADS	• Identify current and emerging risks to Senior Leadership • Oversee risk management by reviewing key risks and response strategies to ensure effectiveness
OPERATIONAL STAFF	• Identify, assess, and evaluate risks to achieve strategic objectives • Set risk priorities for Business Units • Prepare and update risk responses
INTERNAL AUDIT	• Provide guidance and support to divisions • Provide training and education to staff • Facilitate and coordinate the reporting of risks

3. Business Continuity, Technology Disaster Recovery and Cyber Major Incident Risks

In parallel to the ongoing development of Enterprise Risk Management, various initiatives within City Divisions are underway to manage risks in their functional area. Risk management activities are in place within Toronto Emergency Management, Technology Services, and the Office of the Chief Information Security Officer, which collectively aim to address potential gaps to improve the City's ability to maintain critical business functions in the event of a disruptive incident, and to develop strategies to enable continued operations.

Business Continuity Management Program (Toronto Emergency Management)

The Provincial Emergency Management and Civil Protection Act sets the requirements for the City's Emergency Management Program, which include an Emergency Plan that is based on the hazards and risks that could cause an emergency. The Emergency Management Program also includes training, exercises, public education and identifies critical municipal infrastructure that could be impacted during an emergency. The City is compliant with these requirements.

Further to the above emergency management program requirements, the City performs many other processes and activities that will contribute to the larger Enterprise Risk Management program including maintaining the corporate business continuity program, and supporting disaster recovery, and cyber incident response programs in Technology Services and the Office of the Chief Information Security Officer.

Enterprise IT Disaster Recovery Program (Technology Services)

The City's Enterprise IT Disaster Recovery Program establishes the framework and supports policies and standards to maintain the technical aspect of business continuity. Disaster Recovery includes mobilizing a collection of resources and activities to re-establish technology services including infrastructure, telecommunications, systems, applications, and data at an alternate site following a major disruption of critical IT services. In addition, Disaster Recovery encompasses the subsequent resumption and restoration of those operations.

Cyber Incident Response Plan (Office of the Chief Information Security Officer)

The City's Cyber Incident Response Plan provides an overall strategy for responding to cyber security incidents as they occur in the City. It involves detecting, containing and eradicating the incident, investigating its root causes, mitigating the risks, and recovering systems and data. The Cyber Incident Response Plan provides the immediate response measures necessary to minimize the technology impact of the incident on critical business functions and initiate the recovery process.

Joint Program Committee

A Joint Program Committee, consisting of subject matter experts in Toronto Emergency Management, Technology Services and the Office of the Chief Information Security Officer, has been formed to ensure that the three programs above (i.e., Business Continuity Management Program, Enterprise IT Disaster Recovery Program, and Cyber Incident Response Plan) establish a coordinated approach for the City to prepare, respond, and recover from disruptive incidents. These contribute to the holistic enterprise risk management strategies under the City's ERM program.

4. Conclusion

This report outlines the Risk Governance model that oversees Enterprise Risk Management within the City. The City's ERM program is a continuous long-term initiative, which includes integrating the principles contained in the ERM Framework and Policy into business processes. In addition, training and support material will be developed to educate staff and to promote best practice for risk management. In parallel with the City-wide ERM initiative, Toronto Emergency Management, Technology Services and the Office of the Chief Information Security Officer have employed measures to ensure risks are sufficiently managed.

CONTACT

Mala Gautam, Manager, Strategy & Compliance, Technology Services
416-688-4665, mala.gautam@toronto.ca

Ferris Adi, Director, Cyber Diplomacy & Governance, Office of the Chief Information Security Officer, 416-338-1830, ferris.adi@toronto.ca

Tyler Griffin, Manager, Toronto Emergency Management
416-392-3913, tyler.griffin@toronto.ca

Nazma Deen, Acting Manager, Internal Audit
416-338-5962, nazma.deen@toronto.ca

SIGNATURE

Sonia Brar,
Chief Technology Officer

Maneesh Agnihotri,
Chief Information Security Officer

Joanna Beaven-Desjardins,
Executive Director, Toronto Emergency Management

Gifford Chu,
Acting Director, Internal Audit