City of Toronto

Enterprise Risk Management Framework

Last Updated: October 2024

Table of Contents

Purpose of this Document

This document outlines the City of Toronto's Enterprise Risk Management (ERM) Framework which identifies the key elements of the organization's approach to managing risks. The framework provides guidance in how risk management practices can be integrated into business processes at every level of the organization.

The goal is to enhance risk management capabilities within the organization and to build a risk-informed decision-making culture in support of the City's strategic, operational and project objectives, which is fundamental to good management practices and corporate governance.

Definition of Risk and Risk Management

Risk is any barrier or obstacle that prevents the City from achieving its objectives.

Enterprise Risk Management is the holistic approach to proactively identify and manage risks across the organization.

Benefits of Risk Management

The benefits of risk management include the following:

- **Informed decision-making:** better decisions are made when supported by a systematic approach to risk management.
- **Improved resilience:** greater awareness of risks allowing the City to proactively manage and mitigate risks before they materialize.
- **Seizing Opportunities:** fosters agility and the ability to respond effectively to unforeseen challenges or opportunities.

Guiding Principles

The implementation of risk management is guided by the following principles:

- **Simplified:** Risk management should be simple and practical and should not be a laborious administrative process.

- **Integrated:** Risk management should be an integral part of all City-wide activities.

- **Customized:** The use of the risk management framework and supporting tools should be tailored to the City's business and strategic objectives.

- **Collaborative:** Timely engagement of appropriate staff and stakeholders supports improved awareness and more informed risk management.

- **Dynamic:** ERM is fluid and responds proactively to changes in the risk landscape.

Roles and Responsibilities

The following diagram outlines the roles and responsibilities for various levels across the City with regards to ERM:

	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 • Accountable for internal controls across the City
DIVISION HEADS	• Identify current and emerging risks to Senior Leadership • Oversee risk management by reviewing key risks and response strategies to ensure effectiveness • Responsible for the internal controls in their division
OPERATIONAL STAFF	• Identify, assess, and evaluate risks to achieve strategic objectives • Set risk priorities for Business Units • Prepare and update risk responses, operate internal controls
INTERNAL AUDIT	• Provide guidance and support to divisions • Provide training and education to staff • Facilitate and coordinate the reporting of risks • Evaluate internal control design and effectiveness

Integrating Risk Management into City Processes

Risk management should be integrated into activities at all levels of the organization.

- **Decision-making for business operations:** Risk management should be integrated into day-to-day management of activities for informed decision-making with respect to the development and implementation of policies, procedures, processes and programs.

- **Strategic Planning:** Risk management should be directly linked to the City's strategic and business planning to prioritize goals and objectives.

- **Budgeting and planning:** Risk management can be used to assist with decisions regarding resource allocation.

- **Project Management** – Risk management can be used to identify and monitor various risks to the accomplishment of project goals.

- **Reports to Council –** should include disclosure of significant risks associated with alternatives presented and the recommended course of action.

Inclusion of Risk Management Considerations into City-provided Reports to Committee & Council

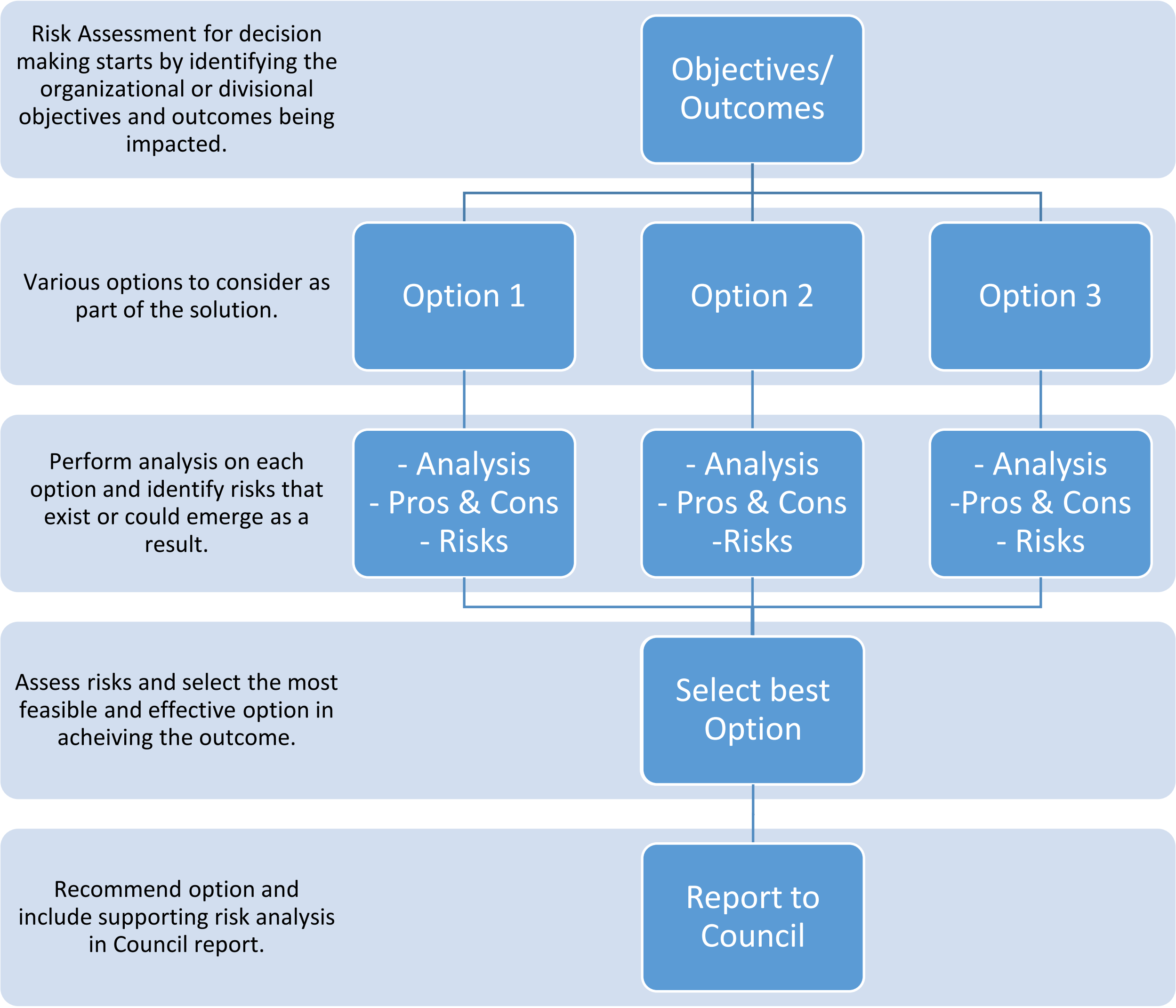
Reports to Council or Committee shall disclose all significant risks associated with alternatives presented arising from activities or recommendations contained in the report. Risk consideration in reports to Council will include risks that:

- The strategy/recommendation aims to address
- The strategy/recommendation introduces
- Could impede the success of the strategy/recommendation
- Will remain unaddressed with the strategy/recommendation

The attached appendices provide guidance in identifying risks and their associated impacts and likelihood, as well as strategies and controls to mitigate such risks.

It should be noted that risk can never be eliminated. It can only be managed to acceptable levels.

Risk Assessment in Decision Making



Risk Assessment for decision making starts by identifying the organizational or divisional objectives and outcomes being impacted.

Objectives/ Outcomes

Various options to consider as part of the solution.

Option 1

Option 2

Option 3

Perform analysis on each option and identify risks that exist or could emerge as a result.

- Analysis
- Pros & Cons
- Risks

- Analysis
- Pros & Cons
-Risks

- Analysis
-Pros & Cons
- Risks

Assess risks and select the most feasible and effective option in acheiving the outcome.

Select best Option

Recommend option and include supporting risk analysis in Council report.

Report to Council

Approach to Embed Risk Management into the Organization

The risk management process can be summarized into 5 main steps as outlined below

1. Objective Setting

- A clear understanding of what is to be achieved and what a successful outcome looks like is necessary.
- Reliance on KPIs, Business Objectives and other Performance Measures can help define the obejctive

2. Identify Risks and Events

- Risks and events that would negatively impact the achievement of objectives should be identified.
- To assist in identifying potential risks, refer to Appendix I and Appendix II for a list of Risk Categories and their definitions.

3. Risk Assessment

- Risks should be assessed to determine if any measures are needed to be put in place to address the risk.
- Assessment includes consideration of the likelihood of a risk occurrence and the impact of a risk on the achievement of the City's objectives. Refer to Appendix III.

4. Methods for Managing Risk

- Based on a risk's impact and likihood, the City will choose to:
  - Avoid the Risk (stop the program or activity)
  - Accept the Risk
  - Reduce the Risk (through internal control activity)
  - Transfer the Risk (through insurance)

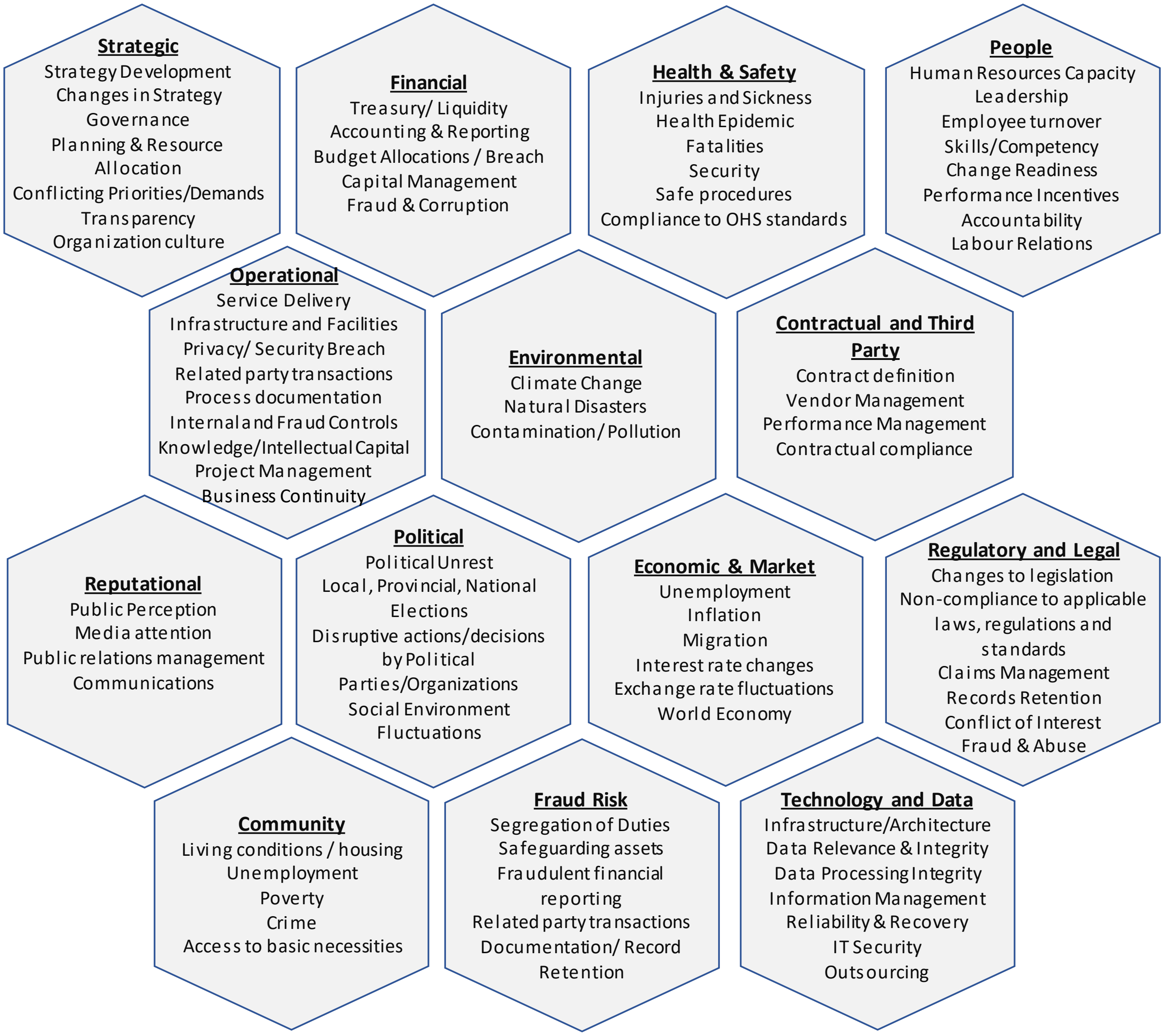
5. Design Mitigation Strategies (Control)

- Actions to mitigate risks are known as internal controls.
- To be successful, they must be cost effective.
- Policies, procedures, planning, direction, supervision and reviews are all examples of internal control
- Refer to Appendix IV for a listing of classifications and categories of controls

Feedback and Updates to Framework

The ERM Framework, and all of its components, will be reviewed at least annually and updated as needed to respond to new risk-oversight needs and any regulatory changes or other requirements. The review will also include comparisons with best practices and consultations with stakeholders.

Appendix I – Risk Categories



Strategic
Strategy Development
Changes in Strategy
Governance
Planning & Resource Allocation
Conflicting Priorities/Demands
Transparency
Organization culture

Financial
Treasury/ Liquidity
Accounting & Reporting
Budget Allocations / Breach
Capital Management
Fraud & Corruption

Health & Safety
Injuries and Sickness
Health Epidemic
Fatalities
Security
Safe procedures
Compliance to OHS standards

People
Human Resources Capacity
Leadership
Employee turnover
Skills/Competency
Change Readiness
Performance Incentives
Accountability
Labour Relations

Operational
Service Delivery
Infrastructure and Facilities
Privacy/ Security Breach
Related party transactions
Process documentation
Internal and Fraud Controls
Knowledge/Intellectual Capital
Project Management
Business Continuity

Environmental
Climate Change
Natural Disasters
Contamination/ Pollution

Contractual and Third Party
Contract definition
Vendor Management
Performance Management
Contractual compliance

Reputational
Public Perception
Media attention
Public relations management
Communications

Political
Political Unrest
Local, Provincial, National Elections
Disruptive actions/decisions by Political Parties/Organizations
Social Environment Fluctuations

Economic & Market
Unemployment
Inflation
Migration
Interest rate changes
Exchange rate fluctuations
World Economy

Regulatory and Legal
Changes to legislation
Non-compliance to applicable laws, regulations and standards
Claims Management
Records Retention
Conflict of Interest
Fraud & Abuse

Community
Living conditions / housing
Unemployment
Poverty
Crime
Access to basic necessities

Fraud Risk
Segregation of Duties
Safeguarding assets
Fraudulent financial reporting
Related party transactions
Documentation/ Record Retention

Technology and Data
Infrastructure/Architecture
Data Relevance & Integrity
Data Processing Integrity
Information Management
Reliability & Recovery
IT Security
Outsourcing

Appendix II – Risk Category Definitions

Risk Category	Risk Category Definition
Strategic Risk	Strategic risks can be defined as the uncertainties and untapped opportunities embedded in the strategic intent and how well they are executed. These risks are evaluated from the perspective of impact they would have on the entire business in relation to the strategic objectives.
Financial Risk	Financial risks include uncertainties and untapped opportunities in effective and efficient utilization of financial resources as well as uncertainties in financial reporting.
Health & Safety Risk	Chance or probability that a person will be harmed or experience an adverse health effect if exposed to a hazard. It may also apply to situations with property or equipment loss, or harmful effects on the environment.
Fraud Risk	Fraud, by definition, entails intentional misconduct, designed to evade detection. As such, the fraud risk assessment should anticipate the behavior of a potential fraud perpetrator.
Operational Risk	Operations risks include risks to efficient and effective utilization of resources (excluding financial resources), and risks resulting from breakdowns in internal procedures, people and systems.
Environmental Risk	Environmental Risk can be defined as the actual or potential threat of adverse effects on living organisms and the environment by natural disasters, effluents, emissions, wastes, resource depletion, etc.
Contractual and Third Party Risk	These risks cover risks arising from poor contract definition with contractors, business partners and vendors as well as risks associated with contractual compliance.
Reputational Risk	Negative public perception and media attention creating a loss of confidence.
Political Risk	Political risk is a type of risk faced by governments that political decisions, events, or conditions will significantly affect the profitability of a business or the expected value of a given economic action.
Economic & Market Risk	Environment and market risks include uncertainties and untapped opportunities arising due to changes in the economy/ market fluctuations or disruptive business models/ innovations.
Technology and Data Risk	Technology risk is any potential for technology failures to disrupt your business such as information security incidents or service outages. Data risk is the potential for a loss related to your data. The term applies to failures in the storage, use, transmission, management and security of data.
Regulatory and Legal Risk	Regulatory risk is the risk of a change in regulations and law that might affect the business. Such changes in regulations can make significant changes in the framework. Legal risk is the potential for losses due to regulatory or legal action.
Community Risk	Community risk consists of factors that impact the community's standard of living, livelihood and way of life. This would also include any barriers to basic services and necessities.
People Risk	People risk, defined as the gap between the goals of the organization and the skills of its workforce. These risks have the potential to impose significant losses on brand, reputation, morale, and revenue.

Appendix III – Risk Impact and Probability Criteria

Risk Impact Scale

	Insignificant – 1	Minor - 2	Moderate - 3	Major- 4	Severe - 5
Financial	Little or no impact on budget.	Able to accommodate within department budget.	Able to accommodate within corporate budget.	Able to accommodate within existing budget but only with service cuts and/or reserve funds.	Unable to accommodate within budget.
Reputational	Little or no impact on level of trust in the City (council and staff). Public reaction minimal - no effect on City's profile.	Adverse/negative view of city (council and staff) is limited to a small area/ community group. Public reaction contained - City's profile raised within local boundaries.	Adverse/negative view of city (council and staff) is held by neighbourhoods/ multiple community groups. Public reaction considerable - City's profile raised within GTA boundaries.	Adverse/negative view of city (council and staff) spans ward boundaries/ majority of community groups. Public reaction major - City's profile raised within provincial boundaries.	Adverse/negative view of city (council and staff) is community-wide. Public reaction severe - City's profile raised within national boundaries.
Operational	Little or no impact on operations/ delivery of all services. No workarounds required to deliver services. No service unavailability.	Minor changes necessary to deliver all services but manageable within complement/ operations. Minor adjustments required to deliver services. Service unavailability of all services for 1 - 2 hours.	Moderate changes necessary to deliver core services, require few additional resources. Workarounds to deliver services are manageable. Service unavailability of core services for several hours.	Major changes necessary to deliver core services, require some additional resources and time to complete. Workarounds to deliver services are complex. Service Unavailability of core services for 1 - 2 days.	Significant changes necessary to deliver core services, require numerous additional resources and extended period of time to complete. No alternatives or workarounds exist to deliver services. Service Unavailability of core services for > 2 days.
People	Little or no impact on staff's performance/ morale. No injury; scare only.	Isolated performance/ morale issues. Minor non-immobilizing injury or trauma not requiring hospital treatment.	Performance/ morale issues found within a department. Non-immobilizing injury or trauma but requiring hospital treatment.	Performance/ morale issues across multiple departments. Immobilizing injury or trauma requiring hospital treatment.	Wide-spread degradation in performance/ morale. Work to rule/ strike. Severe injury or trauma requiring urgent hospital treatment. May be life-threatening or fatal.

Risk Likelihood Scale

	Remote – 1	Unlikely - 2	Possible - 3	Likely - 4	Almost Certain - 5
Description	The event may occur only in exceptional circumstances.	The event could occur at some time but is improbable.	The event might occur at some time.	The event will probably occur.	The event is expected to occur.
Quantification	Should virtually never occur, or occur beyond 10 years.	Unlikely to occur once every 5 to 10 years.	Possible to occur every 2 to 5 years.	Likely to occur every 1 to 2 years.	Almost certain to occur once or more per year.
% Probability	Probability of occurrence is < 5%.	Probability of occurrence is 5% - 35%.	Probability of occurrence is 35% - 65%.	Probability of occurrence is 65% - 95%.	Probability of occurrence is 95% - 100%.

Appendix IV –Internal Control Classifications and Categories

Within an organization, controls can be implemented at various levels:

Entity Level

- Broad procedures that impact the entire organization
- Example include: the code of conduct, overall risk management practices, and performance management.

Process Level

- Specific procedures and actions taken within an organization to manage and reduce risks in particular activities or functions.
- Examples include: approving transactions, verifying data, and maintaining detailed records.

Transaction Level

- Procedures an organization uses to ensure individual transactions are accurate, authorized, and recorded properly.
- Examples include:validating a purchase, approving an expense, or recording a payment, to ensure each transaction is correct and legitimate.

Controls can further be broken down into the following types:

Preventative Controls	Detective Controls	Corrective Controls	Directive Controls
Prevent errors, fraud or undesired events by acting proactively.	Identify and detect errors, fraud or irregulatiies that have occured.	Correcting issues or irregularities that have been detected, focusing on fixing problems	Provide guidance/instruction to ensure activities are carries out as desired.
Examples: Access Controls: Requiring passwords and biometric scans to restrict system access to authorized users only.	Examples: Conducting periodic audits to review and verify the accuracy and completeness of financial or operational data.	Examples: Using data backup and recovery procedures to restore lost or corrupted data.	Examples: Implementing organizational policies that outline the procedures for performing tasks correctly.