STAFF REPORT
ACTION REQUIRED

TTC's Enterprise Risk Management (ERM) Framework

Date:	November 12, 2015
To:	TTC Audit and Risk Management Committee
From:	Chief Executive Officer

SUMMARY

TTC's Enterprise Risk Management Framework (ERM) provides the necessary foundations and organizational arrangements for managing risk across the TTC. It outlines how the TTC ensures that it manages risks effectively and efficiently

The attached presentation summarizes TTC's Enterprise Risk Management Framework and it outlines:

Enterprise Risk Management Framework:

- Purpose
- ERM Policy
- Risk Governance
- ERM Process
- As Low as Reasonably Practicable (ALARP) Principle
- Risk Reporting

Next Steps

Recommendation

1. It is recommended that the Audit and Risk Management Committee endorse the Enterprise Risk Management Framework, including the ERM Policy.

Financial Summary

This report has no financial impact. Ultimately ERM will be used to prioritize funding requirements. The Business Case process will be used should additional resources be required.

Contact

Mohamed Ismail, Principal Risk Advisor
Toronto Transit Commission
Tel: 416 393-2935
Email: Mohamed.Ismail@ttc.ca

Attachments

Enterprise Risk Management (ERM) Framework - Presentation
ERM Policy
ERM Framework

ENTERPRISE RISK MANAGEMENT FRAMEWORK

CONTENT

Enterprise Risk Management (ERM) Framework:

- Purpose
- ERM Policy
- Risk Governance
- ERM Process
- ALARP Principle
- Risk Reporting

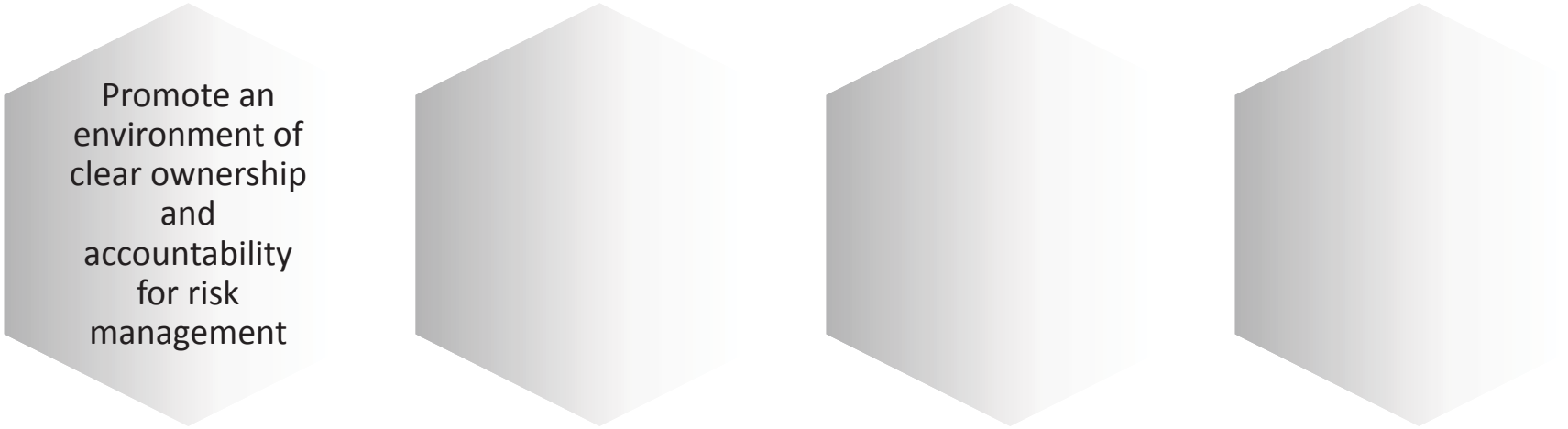
Next Steps

ERM FRAMEWORK - PURPOSE

- Provide the necessary foundations for managing risk across the TTC.
- Outline how the TTC ensures that it manages risks effectively and efficiently.
- Describe the key principles, elements and processes to guide staff in effectively managing risk.

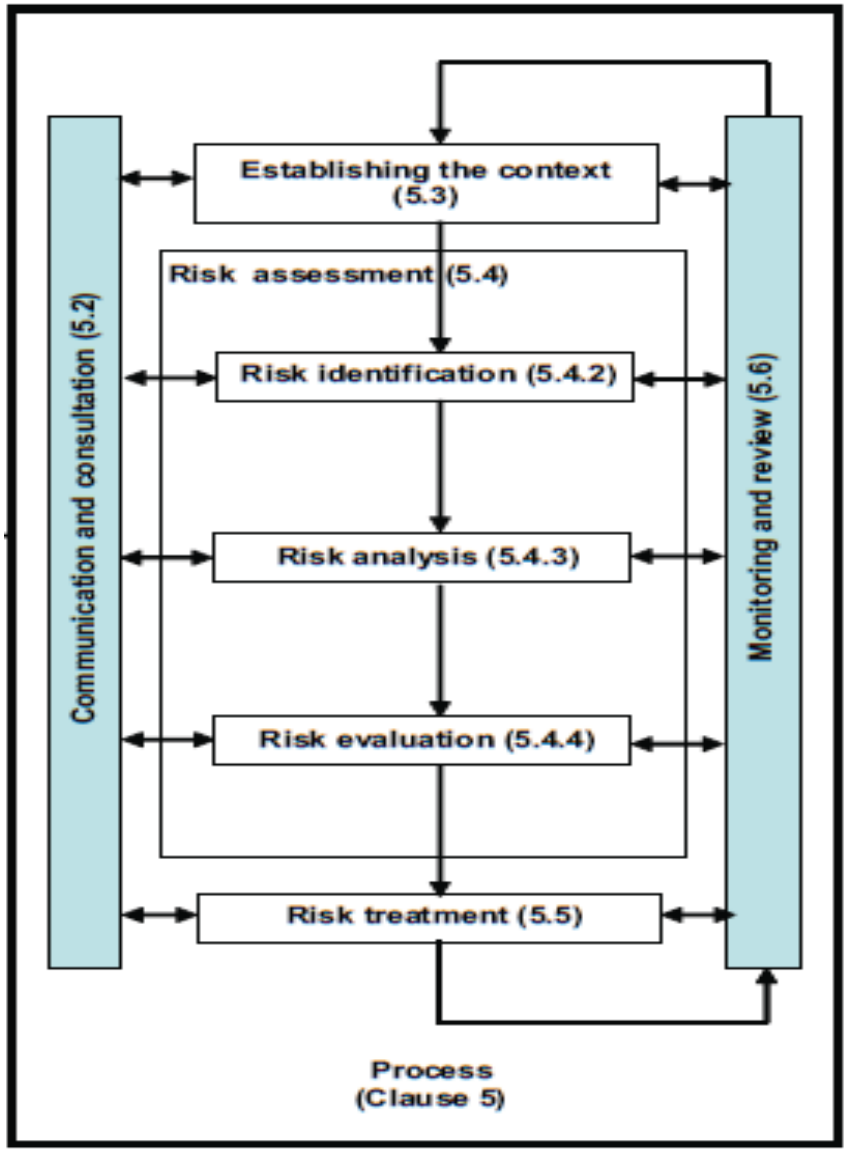
ERM POLICY

The Enterprise Risk Management Policy sets the tone for TTC's commitment to ERM. Ensuring a higher likelihood of success and providing greater confidence and assurance to our customers, employees and stakeholders.



RISK GOVERNANCE

ERM PROCESS

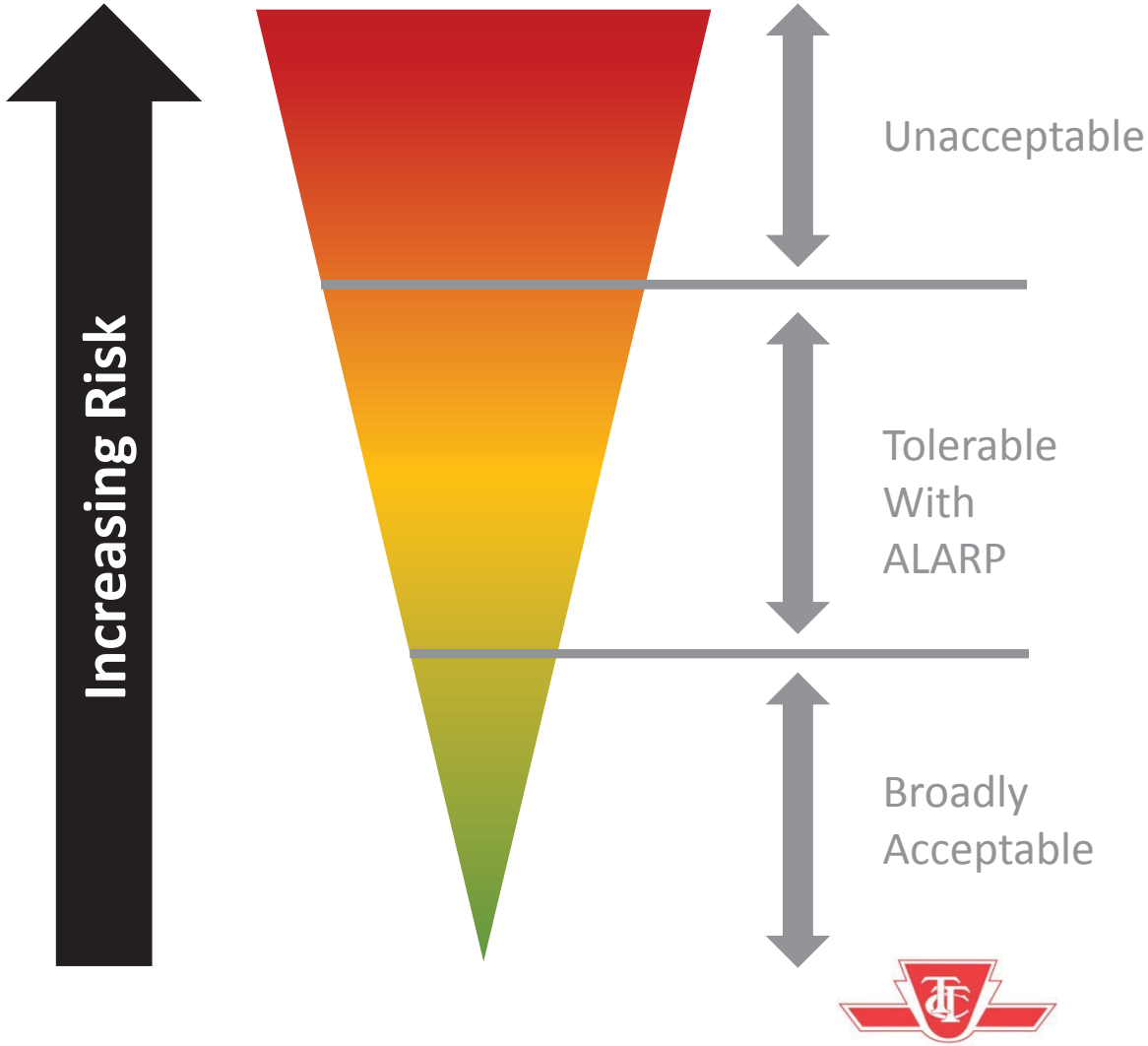


ISO 31000:2009

ALARP PRINCIPLE

As Low as Reasonably Practicable (ALARP):

1. Legal Requirements
2. Contemporary Good Practice
3. Expert Judgment
4. Cost Benefit Analysis



RISK REPORTING

The Audit and Risk Management Committee (ARM) will be provided with quarterly updates on the TTC's Top Risks.

The Risk Management Office will prepare quarterly reports for the Risk and Governance Committee (RGX) to review and the RGX will provide feedback to the risk owners.

NEXT STEPS

Description	Action	Time
February Meeting		
Risk Appetite & Risk Scoring Top 5 Risks Update	Information Information	60 Minutes
May Meeting		
Risk Appetite Statement Top 10 Risks Update	Endorse Information	45 Minutes
July Meeting		
Top 15 Risks Update Issues raised in previous meeting if any	Information	45 Minutes
October Meeting		
Top 20 Risks Update Issues raised in previous meeting if any	Information	45 Minutes

NEXT MEETING

- TTC's Risk Appetite
- How the TTC scores risk
- Top 5 Risks Update

THANK YOU

Questions?

TTC Enterprise Risk Management Policy

Corporate Policy

Creation Date: May 12, 2014
Last Updated: October 8, 2015

TTC Enterprise Risk Management Policy

Purpose

The Toronto Transit Commission's approach to Enterprise Risk Management (ERM) is fundamental to solid management practices and good corporate governance. By understanding and managing the effect of uncertainty on our objectives, we can improve the likelihood of success and provide greater confidence and assurance to our customers, employees, and stakeholders. As the result of a structured approach to risk management, TTC staff and management will be better informed and equipped to recognize and seize on opportunities.

This policy statement communicates TTC's commitment to the use of ERM to ensure the achievement of our strategic objectives.

Policy Statement

TTC will establish, implement and maintain an organization-wide risk management system that supports the achievement of our strategic objectives. We will:

- Integrate ERM into the organization`s culture and business processes;
- Achieve a balance between risk reduction and the cost of risk control;
- Monitor and diligently maintain the integrity and effectiveness of risk controls; and
- Promote an environment of clear ownership and accountability for risk management.

TTC will use a structured and transparent approach to risk management with consistent processes for assessing risks of all types and at all levels across the organization. Risk controls will be implemented where it is reasonably practical to do so and where the cost or impact is proportionate to the expected benefits.

The Audit and Risk Management Committee of the Board (ARM) will ensure TTC maintains a robust ERM framework to manage enterprise risks.

The Risk and Governance Executive Committee (RGX) will oversee the strategic development and on-going implementation of TTC's ERM program.

Risk Owners at the Group and Department levels will continue to have responsibility for managing specific risks. This includes ensuring that the necessary risk controls are in place and are effective at all times, and that control assurance activities are effective.

The Risk Management Office (RMO) will provide assurance of good risk governance through the regular measurement, reporting and communication of risk management performance.

Andy Byford

Chief Executive Officer

TTC Enterprise Risk Management Framework

Creation Date: May 12, 2014
Last Updated: October 8, 2015

Content

1. Introduction

1.1 Purpose

This Framework provides the necessary foundations and organizational arrangements for managing risk across the TTC. It outlines how the TTC ensures that it manages risks effectively and efficiently. It illustrates how risk management is embedded in our organizational systems to ensure it is integrated at all levels and work contexts. It describes the key principles, elements and processes to guide all staff in effectively managing risk, making it part of our day-to-day decision-making and business practices.

The TTC applies risk management across the entire organization. Implementation of the Framework contributes to strengthening management practices, decision making and resource allocation, while at the same time protecting stakeholders' interest and maintaining their trust and confidence.

Implementation of the Framework requires all staff to apply risk management principles to fulfil their responsibilities, to ensure cost-efficient and effective delivery of a transit system that makes Toronto proud.

1.2 What is risk management?

At the TTC, a risk is an event or condition that, if it were to occur, would impact the achievement of the TTC's strategic objectives.

Risk management is a systematic approach with consistent processes for identifying, assessing and controlling risks of all types, at all levels, and for all activities across the organization.

1.3 Benefits of risk management

The benefits of embedding risk management at all levels of the TTC are:

- Effective management of adverse events or opportunities that impact our purpose and objectives;
- Ability to make informed decisions regarding management of potential negative effects of risk and take advantage of potential opportunities;
- Improved planning and performance management processes — enabling us to focus on core business service delivery and implement business improvements;
- Ability to direct resources to risks of greatest significance or impact;
- Greater organizational efficiencies through avoiding 'surprises'; and
- Creation of a positive organizational culture in which people understand their role in contributing to the achievement of objectives.

1.4 Goals of the Framework

The Framework aims to:

- Integrate enterprise risk management within the TTC's Corporate Plan cycle;
- Communicate the benefits of risk management;
- Convey the TTC's policy, approach and attitude to risk management;

- Set the scope and application of risk management within the organization;
- Establish the roles and responsibilities for managing risk;
- Set out a consistent approach for managing risks across the TTC, aligned with relevant standards and industry best practice;
- Detail the process for escalating and reporting risks;
- Convey the TTC's commitment to the periodic review and verification of the Framework and its continual improvement; and
- Describe the resources available to assist those with accountability or responsibility for managing risks.

2. Mandate

2.1 Risk Management Policy

The TTC will establish, implement and maintain an organization-wide risk management program that supports the achievement of corporate objectives. The TTC will:

- Integrate risk management into the organization's culture and business processes;
- Achieve a balance between risk reduction and the cost of risk control;
- Monitor and diligently maintain the integrity and effectiveness of risk controls; and
- Communicate and provide visibility to risk.

The TTC will use a structured approach to risk management with consistent processes for assessing risks of all types, at all levels, and for all activities across the organization. Risk controls will be implemented where it is reasonably practical to do so and where the cost or impact is not disproportionate to the expected benefits.

2.2 Corporate Objectives

The TTC Five Year Corporate Plan defined seven strategic objectives to help realize its vision of a Transit System That Makes Toronto Proud. They are:

Safety: A transit system that manages its risks, that protects its customers, contractors and employees, and that minimizes its impact on the environment.

Customer: A transit system that values customers and provides services that meet or exceed customer expectations.

People: An empowered, customer-focused workforce that values teamwork, pride in a job well done, and an organization that actively develops its employees.

Assets: Effective, efficient management of assets that delivers reliable services in a state of good repair.

Growth: An affordable expansion program that matches capacity to demand.

Financial Sustainability: A well-run, transparent business that delivers value for money in a financially viable way.

Reputation: An organization that is transparent and accountable, well-regarded by stakeholders and peers, in which employees are proud to play a part.

3. A framework for managing risk

3.1 Risk governance

Risk governance includes mechanisms that ensure accountability and authority for the management of risk; implementation, maintenance and continuous improvement of the TTC's risk management framework; and providing risk management assurance. The TTC's governance structure allows for cross group/departmental collaboration and innovation while the governance principles promote the highest standards of ethical behavior and risk management at every level of the organization.

3.1.1 Roles and responsibilities

The Audit and Risk Management Committee

The Audit and Risk Management Committee (ARM) will:

- Review and endorse the TTC's risk appetite statement and related metrics used to define risk tolerances;
- Ensure the TTC maintains a robust enterprise risk management program (ERM) framework;
- Monitor compliance to the ERM framework and its effectiveness for managing risk;
- Review the risk profile and support mitigation plans for the top enterprise risks; and
- Review the system of controls including the establishment and maintenance of business continuity disaster recovery, and emergency management plan.

The Risk and Governance Executive Committee

The Risk and Governance Executive Committee (RGX) will:

- Oversee the development and implementation of a value driven ERM program; and
- Oversee corporate level governance arrangements to aid in effective and efficient decision making.

The RGX shall meet on a monthly basis and otherwise as required. The Committee shall formally report to the Executive Team. This will be done through the issuing of meeting minutes highlights plus any other report the Committee may deem appropriate. The Committee shall report to the Board annually on the TTC's Risk Appetite and TTC's Top Risks.

The Risk Management Office

The Risk Management Office (RMO) mandate is to promote and advance risk management practices at the TTC and to ensure that the system remains fit for purpose. The RMO will:

- Provide tools to appropriately manage risk, coordinate risk management activities and support TTC groups and departments in managing risk;
- Develop and maintain a corporate risk register and risk profile to provide management with the tools and data to make risk-informed decisions; and
- Monitor and report the corporate risk profile and compile risk reports for the RGX and the Executive Team.

Risk Owners

Risk Owners are persons (in positions) with the accountability and authority to manage a risk. This includes ensuring that the necessary risk controls are in place and are effective at all times.

Control Owners

Control owners are persons (in positions) with accountability and authority to implement a specified control and ensure its ongoing effectiveness.

Risk Champions

Each department at the TTC will assign a Risk Champion to:

- Act as the point of contact within their department for the management of risks;
- Coordinate risk assessments and update risk status;
- Work with their team members to ensure risk mitigation actions are being implemented; and
- Work with the RMO to validate and communicate risk changes and updates.

Internal Audit

Internal Audit is responsible for providing independent assessment of the effectiveness of the TTC's processes for managing business risks. The scope of Internal Audit's risk-based program is agreed as part of an Annual Audit Plan which is approved by the Audit Committee.

Project Risk Management

The management of project risks is the responsibility of the Project/Program Manager (PM). Each major project is expected to maintain its own risk register and the PM is expected to actively manage and report risks in a manner that is consistent with the PMI/ISO risk management framework. The Portfolio Management Office (PfMO) and the Risk Management Office (RMO) are available to provide support to PMs in the management and control of project risk.

Employees

Risk Management is every employee's responsibility at the TTC. Here is how employees can do their part:

- Be Knowledgeable about the Risk Management Program, its policy, tools and benefits;
- Identify risks and their impact on the objectives associated with their jobs;
- Manage risks within their own area if possible and understand when to escalate risks or seek additional support if needed;
- Communicate risks through direct reports, risk workshops or the Risk Management Office; and
- Actively participate in risk management activities.

3.2 Risk management process

The risk management process is designed to ensure that risk management decisions are based on a robust approach, assessments are conducted in a consistent manner, and a common language is used and understood across the TTC. Consistent with ISO 31000, the risk management process consists of seven steps, as outlined in Table 1. The TTC's *Risk Management Process* provides a detailed guide to support the effective implementation of the *Risk Management Framework*.

Process Step		Description	Purpose
Communication and Consultation		• Involving stakeholders (internal and external) and information sharing throughout the risk management process, vertically and horizontally across the TTC.	• Context is appropriately defined. • Staff that are involved throughout the risk process understand the basis for decisions and actions required. • Lessons learnt are shared and transferred to those who can benefit from them.
Establish Context		• Understanding the TTC's objectives and defining the external and internal environment within which it operates.	• Understand factors influencing the ability to achieve objectives. • Determine boundaries within which the risk management framework operates. • Define risk criteria to ensure risks are assessed in a consistent manner.
Risk Identification	Risk Assessment	• Identifying risks, its sources, causes and potential consequences.	• Generate a comprehensive list of threats and opportunities based on those events that might enhance, prevent, degrade, accelerate or delay the achievement of objectives.
Risk Analysis		• Comprehending the nature of the risk and determining the level of risk exposure (likelihood and consequence).	• Provide an understanding of the inherent (level of exposure should controls fail) and controlled risk (level of exposure with controls in place). • Assist with identifying ineffective controls. • Inform risk evaluation and guide risk treatment.
Risk Evaluation		• Comparing the risk analysis with the risk criteria to determine whether the risk is acceptable or tolerable.	• Determine whether the controlled risk is acceptable. • Determine if controlled risks need further treatment. • Identify priority order in which individual risks should be treated.
Risk Treatment		• Selecting one or more options for modifying the risk. • Reassessing the level of risks with controls and treatments in place (residual risk).	• Identify treatments for risks that fall outside the TTC's risk tolerance. • Provide an understanding of the residual risk (level of risk with controls and treatments in place). • Identify priority order in which individual risks should be treated, monitored and reviewed.
Monitoring and Review		• Determining whether the risk profile has changed and whether new risks have emerged. • Checking control effectiveness and progress of the treatment plan.	• Provide currency of risk information • Identifying emerging risks. • Provide feedback on control efficiency and effectiveness. • Identify whether any further treatment is required. • Provide a basis to reassess risk priorities. • Capture lessons learnt from event failures, near-misses and success.

Table 1 Risk Management Process

3.3 Risk registers

Risk registers are repositories for risk. Information from the risk management process is recorded, reported and monitored using the department's risk register. Risk registers follow the organizational structure; each department has its own risk register that aggregates up to the group and TTC registers. Risk registers provide access to specified users and govern the actions they can perform.

3.4 Risk Groups

Risk groups are a high level grouping of risks to allow the TTC to have different levels of rating and oversight. There are four Risk Groups which are:

Business Risk Group: This group includes all types of risk except strategic and safety risks. Risks in this group are typically managed at the Department or Group level.

Safety Risk Group: This group includes all safety risks. Risks in this group are typically managed at the Department or Group level.

Corporate Risk Group: This group includes strategic risks in addition to any risk from the safety and business risk groups that exceed the corporate threshold. This threshold is an overall weighted risk score that is established by the RGX and reviewed annually. The current threshold is 200 points.

3.5 Risk Classifications

Risk Classifications are categories of risks that are used to understand sources of risks and decide which risk group it belongs to and where the risk owner should be. There are eight risk classifications as listed in Table 2.

Risk Classifications	Risk Sources	Events/ Examples
Strategic	Strategy/Planning	Unachievable Strategy, Business Model
	Organizational Gaps	Non-existent policies/ processes, Change management
	Governance	Unclear governance/ accountabilities
	Funding	Funding cuts/ Lack of sustainable funding
	Stakeholders & Government	Failure to manage stakeholders/ City relations
Program Delivery	Program delivery	Failure to deliver on a specific program/ initiative
	Capacity Management & Utilization	Lack of capacity/ over-commitment/ underutilization
Operations/ Service Delivery	Asset Management	Asset failure
	Supply-chain management	Critical parts/ material shortages
	Hazards	Events resulting in injury or death
	Service delivery	Service interruptions
	IT	Information management
	Technological	Fail to adopt or implement new technology
Legal & Compliance	Environmental	
	Legal/regulatory compliance	
	Procurement & contract management	
People	Resource management	Skill shortages, Loss of key personnel
	Performance management	Inefficiencies
	Labour relations	Strikes
Security	Terrorism	
	Asset security	Sabotage, Vandalism,
	Crime	Robberies, Assault, Violent crime
	Internal system security	Wilful damage or Theft of information
Financial	Internal fraud	Misappropriation of assets, Bribery, Forgery
	Unauthorized activity	
	External fraud	
	Investment strategy	Fuel hedging
	Financial management	Business and budget planning
Natural disaster & Climate change	Atmospheric Hazards (Severe Weather)	Extreme weather, Ice storms, Flooding
	Geological Hazards	Landslides
	Other Natural Hazards	Epidemics, Pandemics

Table 2 Risk Classifications

3.6 Risk Appetite

Once risks are identified, the adequacy of controls must be considered within the context of the TTC's risk appetite at the time. The TTC risk appetite represents the levels of acceptable and unacceptable risk defined by the Executive Team. The risk appetite reflects the TTC's willingness to take on risk, based on its capacity and its tolerance for potential loss. In addition, risk appetite must be regularly reviewed and approved by the Executive Team.

3.7 Risk reporting

Risk reporting will support management decision making during the planning and review processes. It will also help the TTC monitor the risks and effectiveness of the risk management program.

3.7.1 Risk reports

Risk reports draw information from the risk registers and, depending upon the requirements, may include:

- A demonstration of the link between objectives and risks;
- Priorities, based on the risk rating, accompanied by information on key controls and treatments needed to manage the risk;
- Risks that are getting worse, success of treatment plans and risks that require additional attention;
- New risks that may still need to be fully considered and understood;
- Potential areas that require urgent attention;
- Main areas of exposure;
- Systemic control analysis;
- Untreated risks and risk controls that are overdue; and
- Risk owners.

3.7.2 Corporate risk reporting requirement

- The Risk Management Office (RMO) will receive quarterly updates from Risk Owners including risk status, control implementation and effectiveness;
- The RMO will receive control conformance, control breach and risk tolerance breach alerts;
- The RMO will prepare a quarterly report for the RGX committee to review and the RGX will provide feedback to Risk Owners after their review;
- The RGX will report to the Executive Team as needed; and
- The Risk Management Office (RMO) will provide quarterly updates on TTC's Top Risks to the Audit and Risk Management (ARM) Committee.

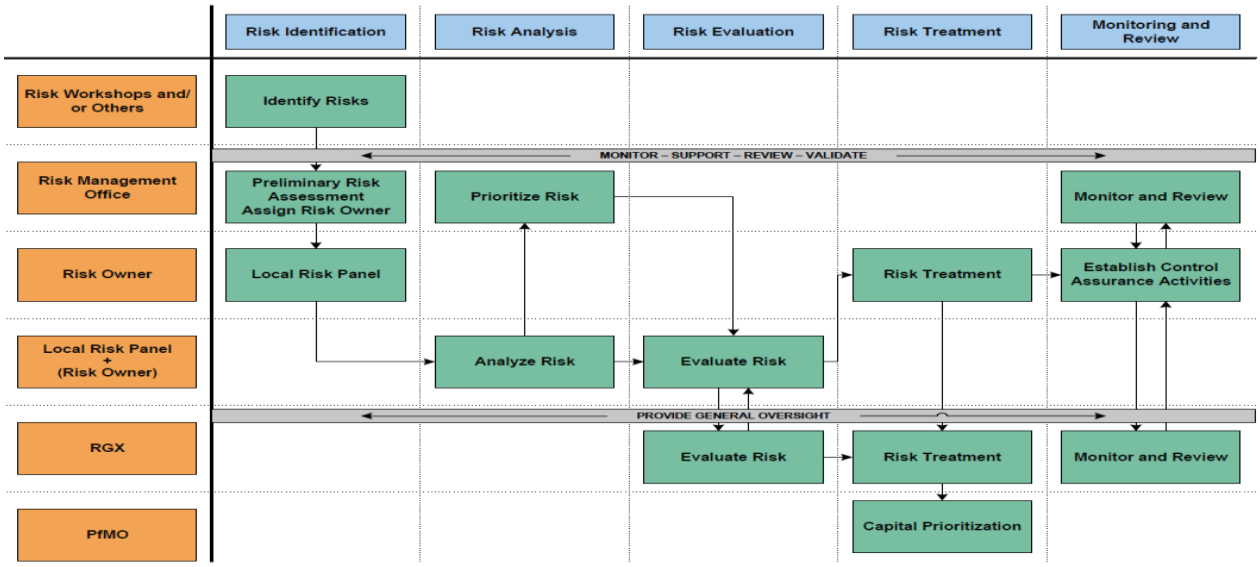
4. Implementing risk management

Risk management should be implemented by ensuring that the risk management process is applied at all relevant levels and functions of the organization as part of its practices and processes, as addressed by Risk management - Principles and guidelines (ISO 31000:2009).

4.1 Risk Management Model

The Risk Management Model below includes key components and processes of implementing risk management at the TTC. It outlines the risk management accountabilities, the structured approach for

identifying, assessing, measuring, mitigating, monitoring and reviewing risks. This model will enable the TTC to manage uncertainty in an effective, efficient and systematic way as well as support continual improvement. It will be applied at all levels of the TTC and to all business activities.



Risk Management Model at the TTC

4.2 Dual assurance and risk bowtie

Risk assessment is a structured approach to identify and analyze the uncertainties that the TTC may face in achieving its objectives. Through the TTC risk management software, the Dual Assurance risk assessment model will be used to asses and manage risks across the whole organization. The Dual Assurance model addresses risk management from two directions:

- The monitoring of controls of a risk to prevent it from eventuating into an incident; and
- Feeding back the lessons learned after the occurrence of an event back into the management of risks.

Risk Bowtie is the selected tool to support risk assessment at the TTC. The Bowtie includes causes, controls, and consequences. For the Dual Assurance risk assessment model, Causes and Prevention Controls must have a contribution percentage.

4.3 Risk Matrix

The risk matrix expresses TTC's tolerance for risk, by making a determination as to the level of risk that is acceptable, based on the combined likelihood of the risk occurring and potential consequences of the risk. This will dictate the points at which risks need to be escalated.

The risk matrix is used to evaluate each identified risk at the TTC. The scales of likelihood and impact are listed in the Risk Ranking Table. There are five color- coded risk levels in the TTC Risk Ranking Table, they are Low, Medium, Serious, High and Very High.

4.4 The ALARP principle

The "As Low as Reasonably Practicable" (ALARP) principle is applied to all potential risks to which the TTC may be exposed. The ALARP principle includes two key elements:

- All efforts should be made to reduce risks to the lowest level possible until the point is reached where the cost of introducing further measures is grossly disproportionate to the benefit that would be achieved; and
- A risk should be tolerated only if it can be demonstrated that there is a clear benefit in doing so.

The ALARP principle identifies three tolerability ranges for risk and the actions needed:

- Very High and High risks are classified as Unacceptable Risk. They must be eliminated or reduced to a level so that it falls into one of the two other levels; or there are exceptional reasons that require the activity or practice;
- Serious and Medium risks are classified as Broadly Acceptable Risk. Further risk reduction is required only if reasonably practicable measures are available; and
- Low risks are classified as Tolerable Risk. They must be properly assessed, controlled and reviewed periodically to keep the residual risk ALARP.

4.5 Risk prioritization

The TTC prioritizes key risks based on their residual and current risk levels. All High residual and current risks will be reviewed periodically with the Risk and Governance Committee (RGX), as well as the Executive Team if needed.

5. Training & Communication

The TTC has clarified roles, responsibilities, accountabilities and authorities at all levels of the TTC. A range of training and development tools are available to build staff awareness and develop skills in 'doing risk management right' and 'doing the right risk management'. This increased awareness and understanding provides staff with greater self-confidence and willingness to take responsibility for the management of risk across the TTC. The TTC Risk Management Framework is embedded in operations through a number of communication, training and support systems, including:

5.1 Training

To ensure that adequate risk management competency levels are achieved and maintained, the TTC will provide regular in class training courses in the risk management process and its application in the TTC.

Specific risk management training sessions are held on quarterly basis, aimed at providing an overview of the Risk Management Framework. The training will be facilitated by the Risk Management Office. Additional ad-hoc training is provided as required.

5.2 Communication

Risk management responsibilities, accountabilities, authorities, processes, trainings and resources are set out in:

- The Risk Management Policy;

- Risk and Governance Executive Committee Terms of Reference;
- RMO's intranet site; and
- Risk registers.

In addition, Advice and support in relation to risk management is available by consulting the department risk champions, Risk Management Office, and the RGX committee.

6. Monitoring, review and continual improvement of the Framework

Continuous improvement is strategically integrated with the TTC's corporate objectives to ensure that the TTC continues to evolve towards best practice. The RGX is responsible for continual improvement of the TTC's risk management, including the *Risk Management Framework*.

Some of the processes that support continuous improvement and review of the Framework include:

- Regular assessment of the quality of risk management processes and risk information prepared by business areas to identify opportunities for improvement;
- Regular reviews of models, frameworks, and standards used in other organizations and jurisdictions to ensure that our Framework continues to reflect contemporary best practice;
- Ongoing training and development for ERM team staff to ensure that the team is equipped with a sound knowledge and skills base; and
- Inclusion of, and measurement against, performance measures relating to the department's performance with regard to risk management and other key governance processes in Corporate Strategy and Performance's operational plan.

The RGX will review the Framework annually and will work with departments to ensure that the Framework and associated business processes continue to meet local needs as risk management matures and improves.

7. References

The Framework is underpinned by Australian and International Standards and a number of evolving best practice guidelines:

- ISO 31000:2009, Risk Management—Principles and Guidelines
- Australian/New Zealand Handbook, Risk management Guidelines—Companion to AS/NZS ISO 31000:2009
- Enterprise Risk Management Framework 2012-2016, Queensland Government
- Risk Management Framework, Griffith University
- TTC Risk and Governance Executive Committee Terms of Reference
- TTC Enterprise Risk Ranking Table