Torres Strait Island
REGIONAL COUNCIL

Torres Strait Island Regional Council
Enterprise Risk Management
Guidelines Document

Contents

Statement of Commitment

The major risk for most organisations is that they fail to achieve their stated strategic business or project objectives or are perceived to have failed by their stakeholders. Torres Strait Island Regional Council (TSIRC) is committed to establishing an environment that is not unduly risk averse, but one that enables risks to be logically and systematically identified, analysed, evaluated, treated, monitored and managed. Risk is inherent in all of Council's activities and a formal and systematic process will be adopted to minimise and where possible eliminate all risks that directly or indirectly impact on the Council's ability to achieve the vision and strategic objectives outlined in the Corporate Plan.

TSIRC is aware that managing risk is not just about avoiding or minimising adverse outcomes, but also has a positive application, in that the proactive analysis of potential risks can also assist the organisation in achieving new and potential opportunities.

This Enterprise Risk Management Guidelines has been developed to demonstrate the Council's commitment, by detailing the integrated Risk Management framework to be employed by all staff members, contractors, committees and volunteers engaged in Council business and defining the responsibilities of individuals and committees involved in managing risk.

In addition, the Guidelines have been developed to:

- Ensure risk management is an integral part of strategic planning, management and day to day activities of the organisation;
- Promote a robust risk management culture within the Council;
- Enable threats and opportunities that face the organisation to be identified and appropriately managed;
- Facilitate continual improvement and enhancement of Council's processes and systems;
- Improve planning processes by enabling the key focus of the organisation to remain on core business and service delivery;
- Encourage ongoing promotion and awareness of the risk management throughout Council.

Introduction

For Council to deliver the strategies and achieve the objectives as outlined in the Corporate Plan, Council needs to identify and manage risks. Risk is an event or action, which has the potential to prevent TSIRC from achieving its corporate objectives. A risk can also be defined as an opportunity that is not being maximised by the Council to meet its objectives.

Enterprise Risk Management (ERM) is the management of risk not only in conventional hazard categories such as health and safety, IT, finance, but in the full spectrum of strategic and operational risk. ERM is the structured approach of aligning strategy, processes, people, technology and knowledge with the purpose of evaluating and managing risk.

Enterprise means the removal of traditional functional, divisional, departmental or cultural barriers. Importantly having a structured approach provides guidance to managing existing and perceived risks that have potential to impact on the organisation's commitment to fulfil its business objectives.

Effective risk management is governed by an organisation's commitment to risk management and this process is outlined in this document which has been developed to align with the Australian Standard AS ISO 31000:2018 Risk management – guidelines.

Definitions

Risk: Risk is defined as effect of uncertainty on objectives. A risk to the business is any action or event that has the potential to impact on the achievement of our corporate objectives.

Risk also arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or that errors will be made.

Risk Management: Risk management for Council refers to the culture, processes and structures developed to effectively manage potential opportunities and adverse effects for any activity, function or process undertaken by the Council. Managing risk is achieved through the systematic application of policies, procedures and practices to identify, analyse, evaluate, treat, monitor and communicate risk.

Enterprise Risk Management (ERM): Enterprise risk management encompasses all the major risk categories (including financial, environmental, health and safety, fraud, information technology, compliance, security and business continuity) and includes the coordination, integration, consolidation and consistency of reporting by the various Council functions with identified risks.

Risk Register: A list of identified and assessed risks directly related to either a department of Council or to the whole of Council. Risk Registers can be held at either Corporate, Operational, Project or Event level.

Likelihood: The chance of something happening, whether defined, measured or determined objectively or subjectively (probability or frequency).

Consequence: The outcome of an event affecting objectives (impact/magnitude). An event can lead to a range of consequences. A consequence can be certain or uncertain and can have a positive or negative effect on objectives. Consequences can be expressed qualitatively or quantitatively.

Risk Owner: The person with the accountability and authority to manage a risk. The owner may delegate some duties in relation to managing the risks for which they are responsible, however they are ultimately accountable for the risks allocated to them.

Risk Treatment: The process to modify existing risks or create new risks. Some options for treating a risk can include: Retaining, Transferring, Sharing, Avoiding or Controlling.

Risk Treatment Action Plans: The document that outlines the steps to be taken to reduce unacceptable risks to achievable and acceptable levels. This includes details on current controls; required risk treatments; improvement opportunities; resources; timing; reporting and accountabilities. Action Plans must be reviewed on a regular basis to ensure controls are working.

Risk Management Principles

For risk management to be effective, an organisation should comply with the following principles.

a) **Integrated** – Risk management is an integral part of all organisational activities

b) **Structured and comprehensive –** A structured and comprehensive approach to risk management contributes to consistent and comparable results

c) **Customised** – The risk management framework and process are customised and proportionate to the origination's external and internal context related to its objectives

d) **Inclusive –** Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

e) **Dynamic –** Risks can emerge, change or disappear as an organisation's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

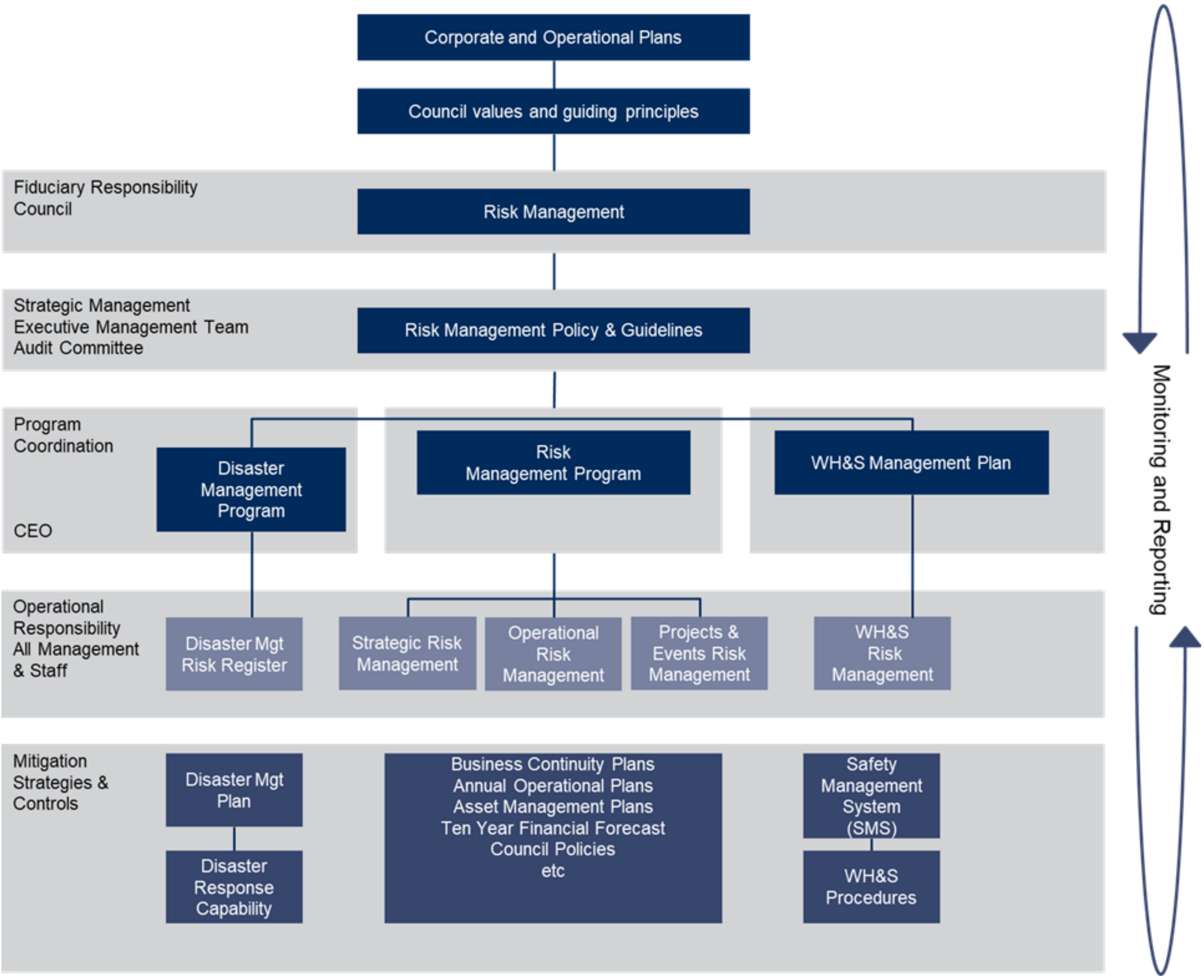
f) **Best available information –** The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly considers any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

g) **Human and cultural factors** – Human behaviour and culture significantly influence all aspects of risk management at each level and stage.

h) **Continual improvement –** Risk management is continually improved through learning and experience.

Risk Management Framework

The Risk Management Framework explains the relationship between the Council's risk management components and other management systems and frameworks.


Corporate and Operational Plans
Council values and guiding principles
Fiduciary Responsibility
Council
Risk Management
Strategic Management
Executive Management Team
Audit Committee
Risk Management Policy & Guidelines
Program
Coordination
CEO
Disaster Management Program
Risk Management Program
WH&S Management Plan
Operational Responsibility
All Management & Staff
Disaster Mgt Risk Register
Strategic Risk Management
Operational Risk Management
Projects & Events Risk Management
WH&S Risk Management
Mitigation Strategies & Controls
Disaster Mgt Plan
Disaster Response Capability
Business Continuity Plans
Annual Operational Plans
Asset Management Plans
Ten Year Financial Forecast
Council Policies
etc
Safety Management System (SMS)
WH&S Procedures
Monitoring and Reporting

Basis, Roles and Responsibilities

Please refer to Council's Risk Management Policy, which describes the roles and responsibilities of the Council, Audit Committee and Employees.

A useful way of describing a risk is to convey an event or situation in terms of what could happen or not happen, or what is present and what it could lead to in terms of consequences regarding the organisation's objectives. This can be applied using the following approach: XXX might occur or not occur, which leads to XXX consequences. This description can also be extended to differentiate between risks, issues and incidents:

	Risk	Issue	Incident
Nature	Nature Variance from desired outcomes	Change in environment, product, system, process or control which means a change in exposures and needs action to prevent incident or loss	An event with impact, whether pre-identified as likely or not
Focus	Future	Present and Future	Present
Effect	Potential loss	Change in risk profile	Actual losses; near misses
Discovery	Deliberate proactive/retrospective identification	Root cause analysis, assurance reviews, self-assessment	Escalation via chain of command
Action Required	Risk Management (assessment, mitigation/controls, monitoring/reporting)	Action planning / Resolution	Immediate response to stop event or minimize losses
Record	Risk Register / Risk Controls	Issue and Action Log	Routine reporting, Incident Log
Reporting	Council, EMT, Department/Functional Managers	EMT, Department/Functional Manager	Employees, Supervisors,Department/Functional Manager

Risk Management Process

The process adopted by TSIRC to manage risks is in accordance with AS ISO 31000:2018 Risk management – Guidelines. This process is the application of the structured risk management methodology to be used to assess; prioritise; treat and monitor risks identified. The risk management process may capture inherent risk (prior to considering controls in place), residual risk (after taking into account controls in place), or both.

The main elements of an effective Risk Management approach are as follows:

- Communicate and Consult
- Establish the Context
- Risk Assessment
- Identify Risks
- Analyse Risks
- Evaluate Risks
- Treat Risks
- Monitor and Review

The following diagram represents the components of the Risk Management process. Each of these components are explained further below.

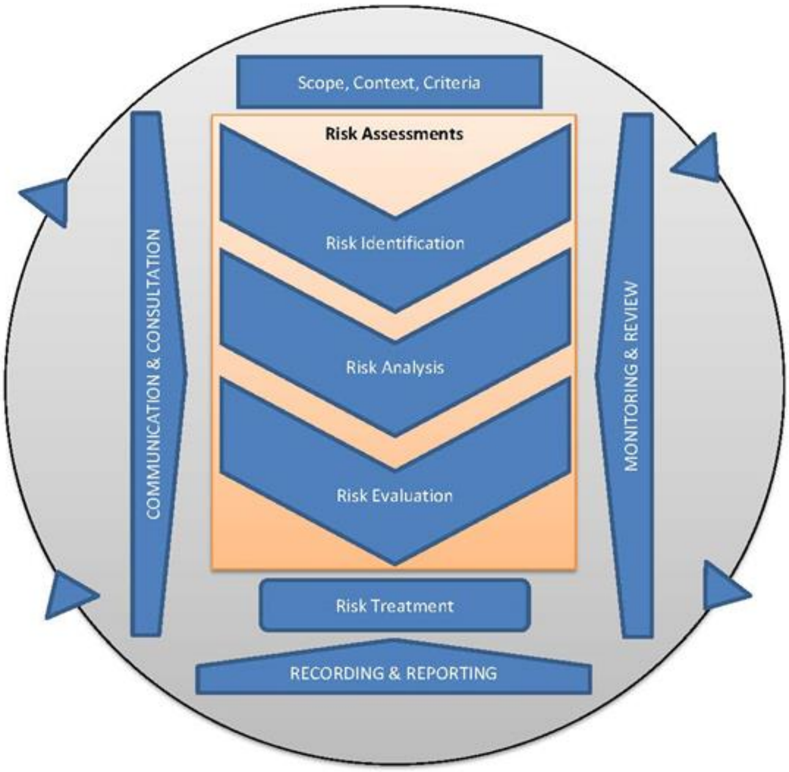


Figure 1 - Source: Australian Standard ISO 31000:2018 Risk management - Guidelines

Communicate and Consult

It is an essential part of the risk management process to develop and implement an effective framework to communicate and consult with all relevant stakeholders, internal and external as appropriate, at each stage of the risk management process and concerning the process as a whole. The level of communication and consultation will vary depending on the level of interest and or influence of that particular stakeholder individual or group. Communication and consultation are necessary at every stage of the Risk Management process.

Establish the Context

Stage one of the process establishes the strategic, organisational and risk management context in which the rest of the process will take place. This includes the criteria against which risk will be evaluated, the risk appetite of the organisation and corrective actions for the different rating achieved in the assessment of the risks.

In considering context, it is necessary to consider the broader external environment in which the organisation operates and not just internal matters.

A written statement of context is to be documented and communicated at the appropriate levels within the organisation.

In establishing the context for these Risk Management Guidelines, existing risk management processes were reviewed, interviews and workshops were held with key personnel and a Risk Management Policy was developed. (Refer to Council’s Risk Management Policy).

Risk Assessment

Risk Identification

At this stage, the organisation identifies what, why and how things can arise, that may affect the organisation, as the basis for further analysis. This is carried out at both strategic and operational levels of the organisation.

Categories of risk for the organisation at a strategic and operational level may include, but are not limited to:

Risk Categories (Exposure Types)	Code,
Infrastructure and Assets Covers infrastructure asset capacity and management (including IT network and hardware), project delivery, inventory and sourcing.	IA
Business Continuity and Business Systems Covers business continuity issues (including IT issues), including those attributable to natural and manmade disasters.	BC
Legal Compliance and Liability Covers legal compliance and liabilities attributable to non-compliance with statutory obligations, including class actions, public liability claims, product liability, professional indemnity and public health and safety.	LL
Reputation Covers Council's reputation with the community, customer service and capability as a regulator.	RE
Political Covers the external political environment in which Council operates, including inter-governmental relations, state and national policies and relations with special interest groups.	PO
Environmental Covers environmental performance of Council's operations including adverse outcomes relating to air, fauna, flora, water, waste, noise & vibration, land, sustainability, hazardous materials and heritage	EN
Finance and Economic Financial and Economic covers financial capacity, availability of capital, the current economic environment, financial management and reporting, knowledge management, efficiency of systems, processes and organisational structure.	FE
Staff Includes human resource, industrial relations and organisational culture particularly relating to staff values, standards of integrity and public accountability.	ST
Workplace Health and Safety	WHS

Covers Workplace Health and Safety issues.	
Climate Change – rising sea level Covers impacts on Council’s assets or infrastructure, erosion or inundation due to sea level rise	CC

Risk Analysis

This stage determines the inherent risks and then calculates any residual risks taking into consideration any existing controls in place (existing processes and procedures). Risks are analysed in terms of consequence and likelihood in the context of those controls. The analysis will consider the range of potential risk exposure consequences and how likely those consequences are to occur. The Consequence and Likelihood are then combined to produce an estimated level of risk known as the Overall Risk Rating.

Determining Likelihood

In determining the likelihood of each risk, the following ratings and definitions have been applied. In making your assessment you have to remember that some events happen once in a lifetime, other can happen almost every day. Judgement is required to determine the possibility and frequency that the specific risk is likely to occur.

Likelihood Table

Short Description	Long Description	Definition - Likelihood of Occurrence/Frequency
Rare	Evidence: Nobody has ever heard of it happening. History: Has not happened previously in our industry, but is a conceivable occurrence. Experience & expectation: Almost sure this won't happen.	Once every 100 years
Unlikely	Evidence: Never heard of it, but it sounds like something that I know has happened elsewhere before. History: Happened previously in our industry. Experience & expectation: I will be surprised if this happened.	Once every 50 years
Possible	Evidence: Similar event occurred, not sure when/where/more than one occasion. History: Logged at least once within our organisation/previous employer(s). Experience & expectation: 50/50 chance that this will happen.	Once every 10 years
Likely	Evidence: Similar event occurred several times over the years. History: Logged several times in our organisation or my previous employer(s). Experience & expectation: I will not be surprised if this happened.	Once every 5 years

Almost Certain	Evidence: People are strongly aware of the risk occurring on several occasions. History: Logged regularly in this area and others on site, a known industry issue. Experience & expectation: Almost sure it will happen.	Once every 2 years

Determining Consequence

In determining the consequence of each risk, the following ratings and definitions have been applied. There are five levels used to determine consequence and when considering how risks may impact on the organisation it is also important to think about the non-financial elements as well.

Consequence Table

Description	Qualitative Definition - Consequence
Insignificant	An event, where the impact can be absorbed; no injuries; low financial loss.
Minor	An event, the consequences of which can be absorbed but management effort is required to minimise the impact; first aid treatment; low-medium financial loss.
Moderate	A significant event, which can be managed under normal circumstances; medical treatment; medium financial loss.
Major	A critical event, which with proper management can be continued; extensive injuries; loss of production capability; major financial loss.
Catastrophic	A disaster, which could lead to the collapse of the organisation; death; huge financial loss.

Quantitative parameters have been developed (Refer Consequence Matrix) to enable the organisation to consistently assign consequence ratings to potential risks. These quantitative measures assign the organisation's risk tolerance parameters applicable to each of the five consequence levels. This approach ensures that all staff can rate the consequence of a risk occurring against the organisation's established parameters, instead of their own personal choice.

Consequence Matrix

Consequence	Rating	Finance and Economic	Human Resources	Infrastructure & Assets	Legal Compliance, Regulatory & Liability (inc. Environment)	Reputation/ Political	Service Delivery	Management Effort/Climate Change Impact
Catastrophic	5	Huge financial loss (e.g. > $1M of revenue or budget)	Fatality or significant irreversible disability. Staff issues cause continuing failure to deliver essential services.	Widespread, long term reduction in service capacity of substantial key assets and infrastructure. Threat to viability of services or operation.	Extensive breach involving multiple individuals. Extensive fines and litigation with possible class action. DLG review or Administrator appointed.	Loss of State Government support with scathing criticism and removal of the council. National media exposure. Loss of power and influence restricting decision making and capabilities.	The continuing failure of Council to deliver essential services. Substantial loss of operating capacity > 1 week. The removal of key revenue generation.	A critical event or disaster that could lead to the collapse of the business
Major	4	Major financial loss (eg. $250,001 to $1M of revenue or budget)	Extensive injuries. Lost time of more than 14 working days.	Widespread, medium to long term reduction in service capacity of key assets and infrastructure.	Major breach with possible fines or litigation. DLG or Administrator may be involved. Critical failure of internal controls may	State media and public concern/ exposure with adverse attention and long-term loss of support from shire residents. Adverse impact	Widespread failure to deliver several major strategic objectives and service	A critical event that with appropriate management can be overcome

			Staff issues cause widespread failure to deliver several major strategic objectives and long-term failure of day to day service delivery.	Loss or event may require replacement of key property or infrastructure.	have significant and major financial impact.	and intervention by State Government.	plans. Long-term failure of Council causing lengthy service interruption up to 1 week.	
Moderate	3	High financial loss (e.g. $50,001 to $250,000 of revenue or budget)	Medical treatment. Lost time of up to 14 working days. Staff issues cause failure to deliver minor strategic objectives and temporary and	Short to medium term reduction in service capacity of key assets and infrastructure. Loss with temporary disruption of key facility and services	Serious breach involving statutory authorities or investigation. Prosecution possible with significant financial impact. Possible DLG involvement. Moderate impact of legislation/regulations	Significant state-wide concern/ exposure and short to mid-term loss of support from shire residents. Adverse impact and intervention by another local government & LGAQ.	Failure to deliver minor strategic objectives and service plans. Temporary & recoverable failure of Council causing intermittent service	A significant event which can be managed under normal circumstances.

			recoverable failure of day to day service delivery.				interruption for a week.	
Minor	2	Minor financial loss (e.g. $10,001 to $50,000 of revenue or budget)	First aid treatment. No lost time. Staff issues cause several days interruption of day to day service delivery.	Minor loss/damage with limited downtime. Repairs required through normal operations.	Minor breach with no fine or litigation. Contained non-compliance or breach with short term significance with minor impact. Some impact on normal operations.	Minor local community concern manageable through good public relations. Adverse impact by another local government.	Temporary and recoverable failure of Council causing intermittent service interruption up to 24 hrs.	An event, the impact of which can be absorbed, but management effort is needed.
Insignificant	1	Low financial loss (e.g. < $10,000 of revenue or budget)	No injury. Staff issues cause negligible impact of day to day service delivery.	Isolated or minimal damage where repairs are required however facility or infrastructure is still operational. .	Isolated non-compliance or breach. Minimal failure managed by normal operations. Insignificant impact of legislation/regulations	Transient matter, e.g. Customer complaint, resolved in day-to-day management. Negligible impact from another local government.	Negligible impact of Council, brief service interruption for several hours to a day.	An event, the impact of which can be absorbed through normal activity

Determining the Overall Risk Rating

After the consequence and likelihood ratings have been determined they are combined in a matrix to determine the overall risk rating for each risk. The extent of the consequences and the extent of the likelihood risks will be assessed using a scale containing Low, Moderate, High and Extreme.

The table below illustrates how the combination of the consequence and likelihood generates the overall risk rating.

Risk Assessment Matrix

		Consequence				
Likelihood	**Rating**	1	2	3	4	5
		Insignificant	Minor	Moderate	Major	Catastrophic
Almost certain	5	M	M	H	H	E
Likely	4	L	M	M	H	E
Possible	3	L	M	M	H	H
Unlikely	2	L	L	M	M	H
Rare	1	L	L	L	M	M

Evaluate Risks

Risks need to be evaluated and prioritised to ensure that management effort is directed towards resolution of the most significant organisational risks first. The initial step in this Risk Evaluation stage is to determine the effectiveness, and or existence of, controls in place to address the identified risks.

This can lead to a decision to: -do nothing further; -consider risk treatment options; -undertake further analysis to better understand the risk; -maintain existing controls; -reconsider objectives.

The following table will assist to determine the effectiveness, and or existence of, controls in place to address the identified risks.

Control Assessment	Description
Excellent	Effective treatments implemented, communicated and monitored on a regular basis to determine the level of effectiveness.
Adequate	Controls are well documented and implemented. The controls address the identified risk and there is little scope for improvement There is no convincing cost/benefit justification to change the approach.
Fair	Controls have been determined, but not well implemented, documented or monitored to determine their level of relevance.

Opportunities for Improvement	Information is inconsistent, not well communicated, implemented in an ad hoc manner. The controls contain some inadequacies and scope for improvement can be identified. There is some cost/benefit justification to change the approach.
Inadequate/Poor	The controls do not appropriately address the identified risk and there is an immediate need for improvement actions. There is a significant cost/benefit justification to change the approach.

Following the process of identification, analysis and evaluation of risks and controls, the outcomes are to be communicated with all relevant stakeholders and agreements reached with the various Risk Owners prior to being documented in the Risk Register.

Risk Register

A Risk Register is developed to record and assess each risk identified as part of the risk identification stage.

The application of the stages of the risk assessment process noted above ensure there is consistency in the determination of the current risk severity level, taking into account the existing controls and their level of effectiveness in mitigating or addressing the risk. Refer to Appendix B for a Risk Register Template.

Risk Profile Diagram

At the completion of the assessment process, a risk profile diagram will be developed to highlight each of the risks identified and their overall risk rating.

The risk profile diagram (example below) will highlight to the CEO and senior executive the key risk exposures and number of risks within each rating range across the organisation. The risks will be categorised as Extreme, High, Medium and Low to assist management to target those risks that have the greatest potential impact on the organisation.

		Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Almost certain	5			1	1	
Likely	4			1	2	
Possible	3		3	1		1
Unlikely	2	2	6	14		2
Rare	1		3			

Treatment of Risks

After evaluating each risk and appropriate controls, it is the responsibility of the manager to implement the suitable treatment. Treatment needs to be appropriate to the significance and priority of the residual risk. As a general guide the following risk treatment options are available:

- **Avoid the risk** - decide not to proceed with the policy, program or activity or choose an alternative means of action

- **Retain the risk –** by informed decision. Where the risk cannot be avoided, reduced or transferred. In such cases, usually the likelihood and consequence are low. These risks should be monitored, and it should be determined how losses, if they occur, will be funded.
- **Transfer or share the risk –** involves shifting all or part of the responsibility to another party who is best able to control it (such as an insurer who bears the consequence of losses e.g. Motor vehicle insurance for Council vehicles).
- **Remove** the risk source
- **Control the risk** – by either reducing the likelihood of occurrence and/or the consequences (e.g. implement procedures for specified tasks
- **Take or pursue the risk –** where a risk presents an opportunity a decision may be taken to enhance, accept, work with or purse the risk.

Determine the most effective treatment options by considering the:

- Cost/benefit of each option including the cost of implementation (do not consider financial considerations only; organisational, political, social and environmental factors should also be considered)
- Use of proven risk controls
- Anticipated level of risk remaining after implementation of risk treatment. The final acceptance of this risk will be a matter for the appropriate Director or CEO to decide.

Once treatment options for individual risks have been selected, they should be assembled into action plans, risk treatment plans or strategies. The outcome of an effective risk treatment plan is knowledge of the risks Council can tolerate and a system that minimises those risks that it cannot tolerate.

The decision to accept a risk will be determined by the agreed table indicating proposed corrective action and the risk appetite criteria established by the Council. For TSIRC a Low risk is accepted and only requires monitoring should circumstances change. For other risks, a specific management plan may be required to be developed and implemented which may include consideration of funding. Risk treatment strategies need to also be considered to ensure that no new risks are introduced.

Escalation Plan

We will introduce procedures for notifying the appropriate persons according to the risk rating, in particular where a risk may escalate due to changed or unforeseen circumstances.

Reports on risk ratings and associated escalation plans will be provided throughout the organisation to assist all staff in managing risk.

The approach for treatment of risks is:

Risk Level	Action Required
Extreme	Immediate action required and must be managed by senior management with a detailed plan
High	Senior management attention needed and management responsibility specified.
Medium	Management responsibility must be specified and response procedures monitored.
Low	Manage by routine procedures at local management level

Monitor and Review

This stage establishes a process to monitor and review the performance of the risk management system implemented and changes that might affect the performance or give rise to new risks that will require assessment.

Both monitoring and reviewing should be a planned part of the risk management process and tailored to the needs of the organisation and the significance of the risks identified. It should be undertaken on at least an annual basis.

The continual process of monitoring and reviewing is required to ensure ongoing effective risk treatments and the continual improvement of the risk management standards.

- ***Monitoring*** – assess whether current risk management objectives are being achieved. Council can use inspections, incident reports, self-assessments and audits to monitor its risk management plan.
- ***Review*** – assess whether the current risk management plan still matches TSIRC's risk profile. The risk management plan may be reviewed by studying incident patterns, legislative changes and organisational activities.

Possible methods for review:

- Internal check program/audit or independent external audit;
- External scrutiny (appeal tribunal, courts, commission of inquiry);
- Physical inspection;
- Program evaluation; and
- Reviews of organisational policies, strategies and processes.

When completing the review process, it is important the context in which the original risk was developed is reassessed. The review should also be informed by reports and recent events and include consideration of:

- Completeness of the register;
- Continued existence of controls;
- Adequacy of controls;
- Risk ratings;
- Treatment strategies;
- Risk owner; and
- Risk review date.

Recording and Reporting the Risk Management Process

The accurate and timely reporting and recording of risks is essential to the effectiveness of the risk management framework. Each stage of the Risk Management process must be recorded appropriately. All Risk Assessments and Risk Treatment Action Plans must be documented, retained and easily accessible for future reference. Even if a risk is assessed to be Low and a decision is taken to do nothing, the reasoning that led to the decision must be recorded.

Reviewing the Risk Management Framework and Guidelines

To ensure that the risk management process is effective and continues to support the organisation's performance, all aspects of the risk management process will be periodically reviewed.

The Risk Management Framework and Guidelines, Risk Management Policy and Risk Registers will be reviewed to ensure that they are still appropriate and continue to reflect the organisation's risk activities and tolerances.

Based on the results of monitoring and reviews, decisions will be made on how the Risk Management Framework can be improved. These improvements should lead to improvements in the management of risk and the risk management culture.

Reporting and Communication

A positive risk culture is one where staff at every level appropriately manage risk as an intrinsic part of their day-to-day work. It is important to ensure that all staff understand, in a way appropriate to their role, what the organisation’s risk strategy is, what the risk priorities are and how their responsibilities in the organisation fit into the risk management framework.

Risk reporting is a key method of communicating risk across the organisation. Regular reports will be provided to the elected Council, Audit Committee, Senior Executive Management Team (EMT) and Departmental/Functional area management. The frequency of reports should be integrated within the ordinary internal reporting cycle, but the significance of the risk must also be considered.

Operational Risks, issues and incidents relevant to a functional area are addressed in the normal team meeting and reporting cycle. Functional managers will be responsible for recording any incidents logged. In circumstances where a change in environment has been identified as needing action to forestall an incident or loss, a report to Executive Management may be required on a more frequent basis until the residual level of risk is acceptable.

The Risk Management Framework and Guidelines, Risk Management Policy, Risk Registers and associated documents and procedures will be held in a secure central repository and will be accessible to stakeholders according to their authority levels. The existence, nature and location of records will be shared with staff at all levels to encourage their awareness of how the organisation is managing its risks.

Reviews of risks, issues and incidents, including any procedural changes will be communicated to the relevant Risk Owners, Risk Action Officers and other stakeholders to ensure that the Enterprise Risk Management process remains dynamic and relevant.

Appendix A – Risk Assessment Template

Enterprise Risk Management – Risk Assessment Template				
Division/Group		Date		
Department		Function/Activity		
Section				
Risk Type		Critical BCP Process		Yes/No

Risk	Risk Category	L	C	Inherent Level of Risk	Inherent Priority Rating	Control Measures	L	C	Residual Level of Risk	Residual Priority Rating

Appendix B - Risk Management Action Plan Template

Risk ID No	Description	Risk Event What might happen?	Source of Risk How might the risk arise?		Resources Required What physical, human or finance resources required?	Performance Measure How will you know the risk treatment is working?	Timeline	Responsibility Name and position

Reviewing Officer:____ Date:________________

Comments:____