muswellbrook shire council

ENTERPRISE RISK MANAGEMENT FRAMEWORK

MSC12E-1

Contents

INTRODUCTION

Background

The purpose of the Enterprise Risk Management (ERM) Framework is to establish a consistent and structured approach to risk management with the aim of assisting Muswellbrook Shire Council (Council) to achieve its objectives and embed risk management in all key operational processes.

Council is exposed to significant uncertainties impacting the delivery of services and achievement of objectives for the community. Significant risks include:

- Increasing operating costs and increasing community expectations for service delivery in a rate-capped environment;
- Global financial trends with local implications – affecting employment, tourism, events, property values, rate income levels and people's ability to pay rates;
- Expectations of greater levels of community engagement, consultations and participation in decision making;
- The challenge of managing Council's ageing assets in a cost effective manner;
- The impact of climate change on Council assets, the community and the environment;
- The need to provide varied and increased services for an ageing population; and
- Council's ability to attract and retain skilled employees.

The ERM Framework provides a foundation for responding to these uncertainties through a structured approach that facilitates risk-informed decision making aligned with Council's strategic, operational and project-specific objectives.

Mandate & Commitment

Council is committed to effectively and systematically managing risks in order to maximise opportunities and limit effects in accordance with *AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines.*

Council recognises that risk is inherent in all Council activities and processes and that ERM is essential for the efficient and effective governance of the organisation in its delivery of services to the community. Council also recognises that risk management cannot eliminate all risks, but will enable the management of risks to an acceptable level.

Council will integrate a structured approach to the management of risk throughout the organisation in order to promote and demonstrate good corporate governance, to minimise loss and to maximise opportunities to improve service delivery and customer value.

Council recognises that an organisation without a robust system for managing risks is vulnerable to uncertainties and lost opportunities and is unlikely to be resilient in the face of change or diversity.

Objectives

Council will seek to meet the principles of risk management as listed in *AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines* with the objectives that risk management:

- Creates and protects value;
- Is an integral part of organisational processes;
- Is part of decision making;
- Explicitly addresses uncertainty;
- Is systematic, structured and timely;
- Is based on the best available information;
- Is tailored;
- Considers human and cultural factors;
- Is transparent and inclusive;
- Is dynamic, iterative and responsive to change; and
- Facilitates continuous improvement of the organisation.

ROLES AND RESPONSIBILITIES

Councillors

Councillors are responsible for making informed decisions that take the associated risks and opportunities into consideration. They must recognise the need to resource the management of risk in order to achieve Council's objectives.

General Manager

The General Manager is responsible for the implementation of the Risk Management Framework, and for ensuring that risks are effectively managed across all activities.

This includes:

- Supporting, promoting and participating in Council's Risk Management Program
- Ensuring that adequate resources are available to support effective and efficient risk management throughout the organization
- Advising the Council on risks and opportunities, as appropriate
- Ensuring that risk management activities are aligned with Council's strategies and objectives.

Manex

Manex are responsible for driving risk management across the organisation and for the implementation within their respective areas of accountability in line with *AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines.* They are responsible for allocating appropriate resources for the implementation and maintenance of the risk management system, to assign responsibilities and accountabilities to managers and individual employees and to establish key performance measures for the management of risk across the organisation. They have responsibility for the development, ongoing review and refinement of strategic risks as well as operational risks within their areas of accountability.

Directors

The Director Environment and Community Services and Director Community Infrastructure are responsible for:

- Supporting, promoting and participating in Council's Risk Management Program in relation to the functions and services in their respective areas of responsibility
- Ensuring that adequate resources are available to support effective and efficient risk management in their respective areas of responsibility
- Actively contributing to the development and implementation of a strong enterprise risk mangement framework and risk management culture within their respective areas of responsibility
- Ensuring that any operational decisions and recommendations go to Council and have appropriate regard to risk management
- Identifying and managing risks in their respective areas of responsibility, in accordance with this framework, and all relevant policies and procedures
- Keeping the General Manager informed of any major risks or significant changes to the risk profile in relation to the delivery and their respective areas of responsibility.

Manager Integrated Planning, Risk and Governance

Reporting to the General Manager, the Manager Integrated Planning Risk and Governance is responsible for the coordination, development and implementation of Council's corporate governance framework, enterprise risk management, policy development, business development, business planning, privacy management and business continuity planning.

This includes:

- Developing and implementing a strong Enterprise Risk Management Framework and risk management culture within Council
- Adopting a strategic approach in relation to Council's corporate governance and risk management

- Remaining abreast of contemporary practices to drive improvement and cultural change
- Coordinating and providing information to the Audit, Risk and Improvement Committee to ensure effective outcomes as per the respective committee charters
- Coordinating Council's internal audit program
- Developing, maintaining and providing guidance in relation to Council's corporate risk register (including the coordination of regular, systematic reviews)
- Providing advice, guidance and recommendations to staff at all levels in relation to the effective management of risk.

Section Managers

Section Managers are responsible for:

- Supporting, promoting and participating in Council's Risk Management Program in relation to the functions and services in their respective section
- Participating in the development of the corporate risk register and undertaking regular, systematic reviews of the risks relating to delivery of their respective section's functions
- Identifying and managing risks in relation to delivery of their respective section's functions, in accordance with this framework and all relevant policies and procedures
- Ensuring that adequate resources are available to support effective and efficient risk management in their respective section
- Ensuring that any operational decisions and recommendations go to Council and have appropriate regard to risk management
- Keeping senior management and the Manager Integrated Planning, Risk and Governance informed of any major risks or significant changes to the risk profile in relation to the delivery of their respective section's functions.

Project Managers

Project Managers are responsible for:

- Supporting, promoting and participating in Council's Risk Management Program in relation to their role
- Developing a project risk register and undertaking regular, systematic reviews of the risks relating to delivery of their projects
- Identifying and managing risks in relation to delivery of their projects, in accordance with this framework and all relevant policies and procedures
- Ensuring that adequate resources are available to support effective and efficient risk management, as part of project planning
- Actively contributing to the development of a strong risk management culture within their project teams

- Ensuring that any operational decisions and recommendations go to Council and have appropriate regard to risk management
- Keeping senior management and the Manager Integrated Planning, Risk and Governance informed of any major risks or significant changes to the risk profile in relation to the delivery of their respective section's functions.

Audit, Risk and Improvement Committee (ARIC)

The Audit, Risk and Improvement Committee are responsible for providing independent assurance to the Council in relation to risk management, internal control, governance and external accountability procedures, in accordance with its Charter.

The ARIC is responsible for reviewing and providing advice to management regarding:

- Council's compliance with relevant risk management standards
- Council's risk management framework and procedures for identification and management of business and financial risks, including fraud
- Council's approach to developing risk management plans for major projects or undetakings
- Council's business continuity planning and preparedness
- The impact of the risk management framework on Council's control environment and insurance arrangements.

All staff, contractors and volunteers

All staff, contractors, volunteers and persons engaged to perform functions of Council are responsible for:

- Supporting, promoting and participating in Council's Risk Management Program within the scope of their influence and position description
- Identifying, managing and escalating risks in relation to delivery of their respective functions in accordance with this framework and all relevant policies and procedures
- Ensuring that any actions taken have appropriate regard to risk management.

RISK MANAGEMENT PROCESS

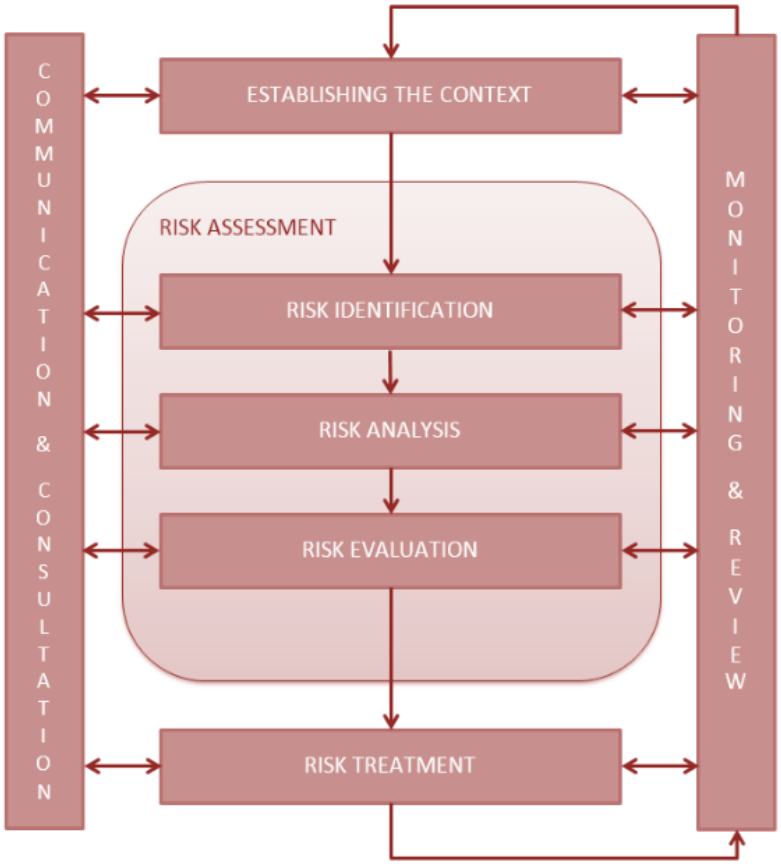
General

At Council, managing risk means actively coordinating activities to direct and control risk within Council and allowing the process to better enable Council to meet its objectives. Council's ERM Framework defines a consistent and structured approach for Council's risk management process that aligns with the requirements of *AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines.*

The following terms, as defined in *AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines,* will apply:

- **Risk –** the effect of uncertainty on objectives;
- **Risk Management –** the coordinated activities to direct and control an organisation with regard to risk;
- **Risk appetite –** amount and type of risk that an organisation is willing to pursue or retain;
- **Risk criteria –** terms of reference against which the significance of a risk is evaluated;
- **Risk assessment –** overall process of risk identification, risk analysis and risk evaluation;
- **Control –** measure that is modifying risk;
- **Risk register –** record of information about identified risks;
- **Risk profile –** description of any set of risks; and
- **Risk reporting –** form of communication intended to inform particular internal and external stakeholders by providing information regarding the current state of risk and its management.

The risk management process is illustrated below.



ISO 31000 (2009)

The five (5) key steps of the risk management process are:

- Communication and consultation;
- Establishing the context;
- Risk assessment (identify, analyse and evaluate risks);
- Treating risks; and
- Monitoring and review.

Communication and Consultation

Communication and consultation with relevant internal and external stakeholders are important elements at each step of the risk management process. Effective communication is essential to ensure that those responsible for implementing risk management and those with a vested interest understand the basis on which risk management decisions are made and why particular actions are required.

Where appropriate, consulting stakeholders with different experiences, beliefs, assumptions, needs and concerns about the risk ensures thorough and comprehensive consideration of the risk being assessed.

To ensure the currency, validity and usefulness of the integrated risk management program, we will provide risk reports to key stakeholders as detailed below:

Council – Council will consider reports concerning risk management from the Audit, Risk and Improvement Committee and give due consideration to risk management issues raised in Council reports.

Audit, Risk and Improvement Committee – The Audit, Risk and Improvement Committee will review Council's Enterprise Risk Management Framework, Strategic Risk Register and Business Continuity Plan to ensure the adequacy of our processes for managing risks.

Manex – Manex will review reports to Council and determine whether risks and risk treatments identified in reports to Council should be subject to further analysis and/or included in Council's risk database.

Establishing the Context

Establishing the context requires an examination of the external, internal (or organisational) and risk management environments in which risk identification, analysis and treatment options will be considered.

Establishing the external context is not only about considering the external environment, but also includes the relationship or interface between the Council and its external environment. This may include:

- Business, social, regulatory, cultural, competitive, financial and political environments;
- International, National and State industry trends and practices;
- Community trends;
- Council's strengths, weaknesses, opportunities and threats (SWOT); and
- Strategic relations with external bodies.

An understanding of Council as an organisation is important prior to understanding the risk management process, regardless of the level. Areas to consider include:

- Goals and objectives and the strategies that are in place to achieve them;
- Organisational culture;
- Strategic drivers;
- Internal stakeholders;
- Organisation structure; and
- Organisational resources such as people, systems and processes.

Council has established a number of risk categories. The risk categories reflect the types of risk consequences to which Council is exposed, and are integrated into Council's risk assessment process as defined in the Guideline. The risk categories will be applied to sort risks as a basis for comparison, reporting and decision making.

Risk Appetite

Council accepts that there is risk in all operations and functions and that the risk appetite will vary depending on the category of risk. Council recognises that in some instances it will have a higher appetite for risk in order to achieve its objectives and capitalise on opportunities.

Council will be required to accept some level of well managed risk which may remain residual in the following areas:

- Supply and improvements to community services;
- Improved efficiency and effectiveness of Council's operations;
- Where the cost of mitigating risk is grossly disproportionate to the evaluated loss; and
- When short term resistance may be experienced but long term gains are expected.

Council will have a lower appetite for residual risks that may foreseeably:

- Compromise the health, safety and wellbeing of people whether they be employee's partners or members of the community; or
- Where risk taking clearly contravenes legislation.

All hazards shall be eliminated as low as reasonably practicable (ALARP). If it is not practicable to eliminate the hazard then additional controls should be put in place to minimise the risk in accordance with the risk to a tolerable level (See Risk Evaluation for more information).

- Keeping senior management and the Manager Integrated Planning, Risk and Governance informed of any major risks or significant changes to the risk profile in relation to the delivery of their respective section's functions.

	Low Risk Appetite Preference for options that avoid risk or have low inherent risk **Minimal**	**Medium Risk Appetite** Preference for safe options with low degree of residual risk and limited potential for reward **Cautious**	**High Risk Appetite** Willing to consider all options with preference for sensible options and an acceptable level of reward **Open**	**Extreme Risk Appetite** Enthusiasm for innovation leading to preference for higher rewards despite greater inherent risk **Seeking**
People	✓			
Environmental	✓			
Assets	✓			
Compliance	✓			
Financial	✓			
Reputation		✓		
Operations			✓	
Technology & Systems			✓	

Risk Identification

Risk identification is the process of identifying risks facing Council. This involves thinking through the sources of risks, the potential hazards, the possible causes and the potential exposure. The risk identification process should be systematic and comprehensive and should include those risks not directly under the control of Council.

The key questions when identifying risks are:

- What can happen?
- Where can it happen?
- When can it happen?
- Why can it happen?
- What is the impact?
- Who is responsible?

It's important to capture the identified risk in a manner that allows it to be fully understood by all stakeholders. In accordance with AS/NZS ISO 31000:2009, the wording to be used to describe a risk within Council is:

"There is a risk that (*something might occur or not occur or is present*) which leads to (*consequences with reference to particular objective*)".

The description can be extended to say what causes the risk and how the consequences might arise.

A variety of methods can be used to identify risks including:

- workshops;
- audits;
- physical inspections;
- brainstorming;
- examination of local or overseas experience;
- expert judgement;
- flow charting, business process reviews;
- interview/focus group discussion;
- operational modelling;
- past organisational experience;
- scenario analysis;
- strengths, weaknesses, opportunities and threats (SWOT) analysis;
- work breakdown structure analysis;
- review of incidents;
- periodic reviews of the risk register; and/or
- bow tie charts.

Risk Analysis

Risk analysis involves consideration of the causes and sources of risk, their potential consequences and the likelihood of those consequences occurring. Consequence and likelihood are combined to

produce an estimate of the level of potential risk. Risks should be considered in the context of existing controls.

Consequence Descriptors

Impact Category	Consequence Severity Level				
	1	2	3	4	5
People	No treatment required	First Aid Only	Medical Treatment Restricted Work Case Lost Time Injury	Significant injury or long term illness; hospitalisation	Fatality; Permanent disability, illness or disease.
Environmental	Little or no environmental harm e.g. minor spill on dirt / road immediately cleaned up or sediment generation.	Minimal environmental harm e.g. erosion within site, dust generation staying on site, small amount of sediment leaving site.	Moderate environmental impact e.g. over-clearing, moderate amount of sediment in waterway, dust impacting areas off site	Significant environmental harm. e.g. large amount of sediment in waterway, damage to cultural site.	Major environmental harm. e.g. major pollution causing significant damage to environment, multiple fauna deaths.
Assets	Minor loss sustained; no repair or replacement required.	Minor damage or insignificant loss; loss is within insurance excess.	Moderate damage or loss; replacement or repair within 6 months.	Major damage or significant loss; Complete replacement or rectification within 6 -12 months.	Catastrophic damage or total loss; Asset written off; Replacement timeframe ≥ 1 year.
Compliance	Isolated non-compliance or breach; minimal failure of controls.	Contained non-compliance or action with short term significance; minimal impact on normal operations.	Significant claim or breach involving statutory authority or investigation; possible prosecution.	Major breach with litigation/fines and long term significance; critical failure of controls.	Extensive litigation/fines with possible class action; indictable offences.
Financial	Negligible financial loss; less than $10,000; up to10% of program/project value.	Minor financial loss; $10,000 - $50,000; 10% - 15% of program/project value.	Significant financial loss; $50,000 - $500,000; 15% - 25% of program/project value.	Major financial loss; $500,000 - $1m; 25% - 50% of program/project value.	Extensive financial loss; in excess of $1m; >50% of program/project value.
Reputation	Minor community concerns and criticism; minimal attention.	Heightened local community concerns and criticism; Internal or partnership attention.	Significant public criticism with our without media attention; short to mid-term loss of support from community.	Serious public outcry, state media attention and long term loss of support from community.	Extensive public outcry; national media attention; loss of State government support with appointment of administrator.
Operations	Minor backlog of operational activities.	Contained impact on operations of short term significance.	Significant impact on service delivery involving investigation.	Major impact on critical operations with long term significance.	Extensive and/or total loss of operations. Disaster management required.
Technology & Systems	No measurable operational impact.	Minor downtime or outage in single area of the organisation; addressed with local management and resources.	Significant downtime or outage in multiple areas of the organisation; substantial management required.	Loss of critical functions across multiple areas of the organisation; long term outage; extensive management with external resources required.	Extensive and/or total loss of operations. Disaster management required.

Likelihood Descriptors

LIKELIHOOD		
A	Almost Certain	It is expected to occur more than once a year.
B	Likely	Will probably occur at least once a year.
C	Moderate	Could occur at some time; possibly once every 5 years
D	Unlikely	Could occur at some time; possibly once every 10 years
E	Rare	May occur only in exceptional circumstances

Level of Risk

	Consequence Severity Level				
	1	**2**	**3**	**4**	**5**
A	Medium (11)	High (16)	High (20)	Extreme (23)	Extreme (25)
B	Medium (7)	Medium (12)	High (17)	High (21)	Extreme (24)
C	Low (4)	Medium (8)	High (13)	High (18)	High (22)
D	Low (2)	Low (5)	Medium (9)	High (14)	High (19)
E	Low (1)	Low (3)	Medium (6)	Medium (10)	High (15)

Risks can be assesses from:

Inherent (Initial) Risk – overall raw, untreated risk or worst case scenario. It is determined by combining the likelihood and consequence ratings without reference to any existing controls.

Residual Risk – level of risk in light of existing controls. Ultimately, the level of risk will determine how a risk is treated.

Proposed Risk – level of risk that would remain if the additional or proposed controls were to be successfully implemented. For risks where the decision is made to accept the risk, the proposed risk level will be the same as the residual risk level.

Risk Evaluation

Risk evaluation involves comparing the level of risk found during the analysis process against the risk criteria to determine whether the risk is acceptable. It involves making decisions based on the risk rating about which risks are going to be treated and the priorities of those treatments. Treatment strategies will vary depending on the level of risk. It's important to strike a balance between the cost of eliminating or reducing a risk and any potential benefits or loss reduction.

The higher the overall level of risk the greater level of management attention is required to reduce its probability and/or impact or manage the risk.

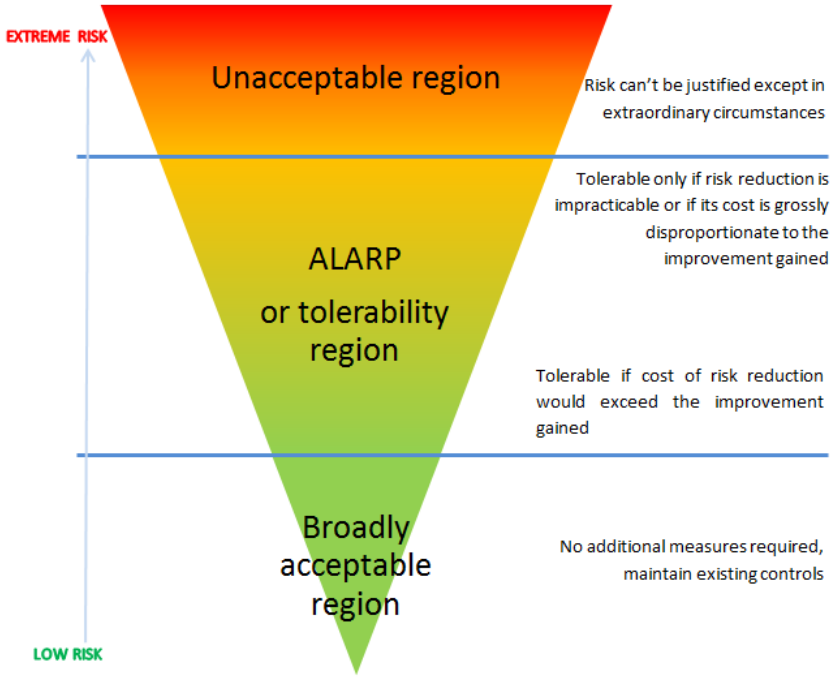
The ALARP (As Low As Reasonably Practicable) principle covers two main areas of risk—acceptability and tolerability. It involves weighing a risk against the effort, time and resources needed to control it.

Application of the concept provides a better understanding of the level and significance of risks and, in turn, can be used to provide support in decisions relating to risk control measures. The application of this principle revolves around the following key aspects:

Intolerable region: an upper level above which risk is intolerable

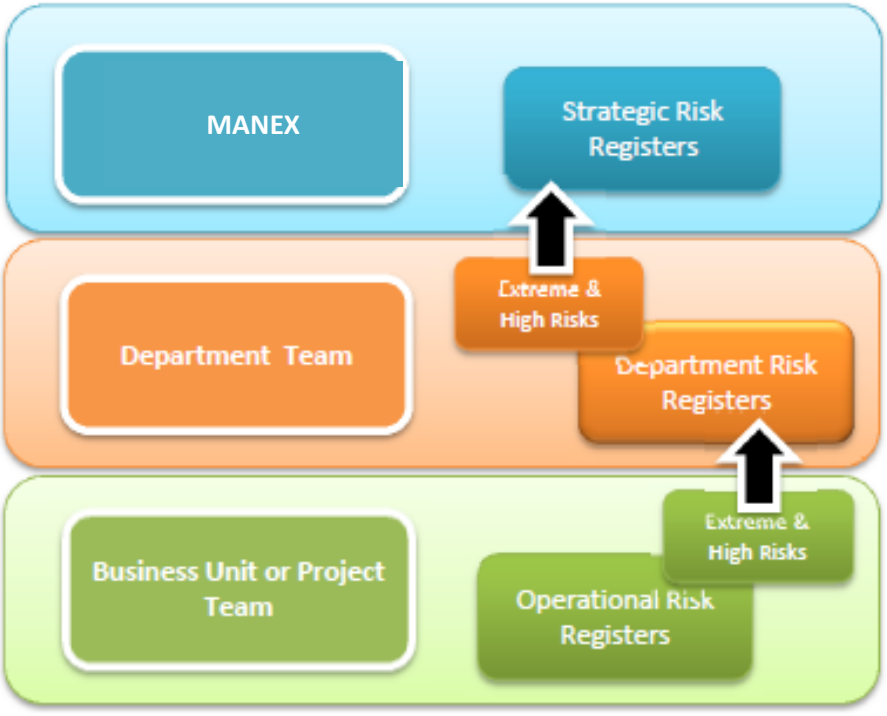
Broadly acceptable region: a lower level below which the risk is broadly acceptable without further treatment as it is very small

Tolerable region: a region between the upper and lower level where risk is tolerable providing it has been reduced to a level which is ALARP (as low as reasonably practicable)



Because Council's Risk Management Framework allows for risks to be assessed against criteria which are appropriate to the size of risk faced by individual sections, it's important to identify those risks which need to be monitored and controlled at a Department and/or organisational level. To achieve this, an escalation model is used whereby risks identified as "Extreme" or "High" at the Section, Business Unit or project level must be re-assessed at Department level as illustrated below. Similarly, those risks identified as "Extreme" or at a Department level must be escalated to MANEX to be re-assessed at an enterprise, or whole of organisation level.

RISK RATING	ACTION	RESPONSIBILITY FOR ACTION
EXTREME	▪ Bring to the attention of the Director for immediate management action ▪ All possible treatments must be put in place to reduce the risk to an acceptable level ▪ Report quarterly to MANEX	Director
HIGH	▪ Bring to the attention of the Manager for immediate management action ▪ Allocate actions and budget to minimise risk ▪ Report quarterly through the Audit Committee	Manager
MEDIUM	▪ Identify management responsibility, monitor and review response action as necessary ▪ Allocate resources where existing controls are deemed inadequate ▪ Report to Audit Committee annually	Coordinator / Supervisor
LOW	▪ Accept and monitor ▪ Manage through existing processes and procedures ▪ Report via routine internal reporting mechanisms	Coordinator / Supervisor



Risk Escalation Model

Risk Treatment

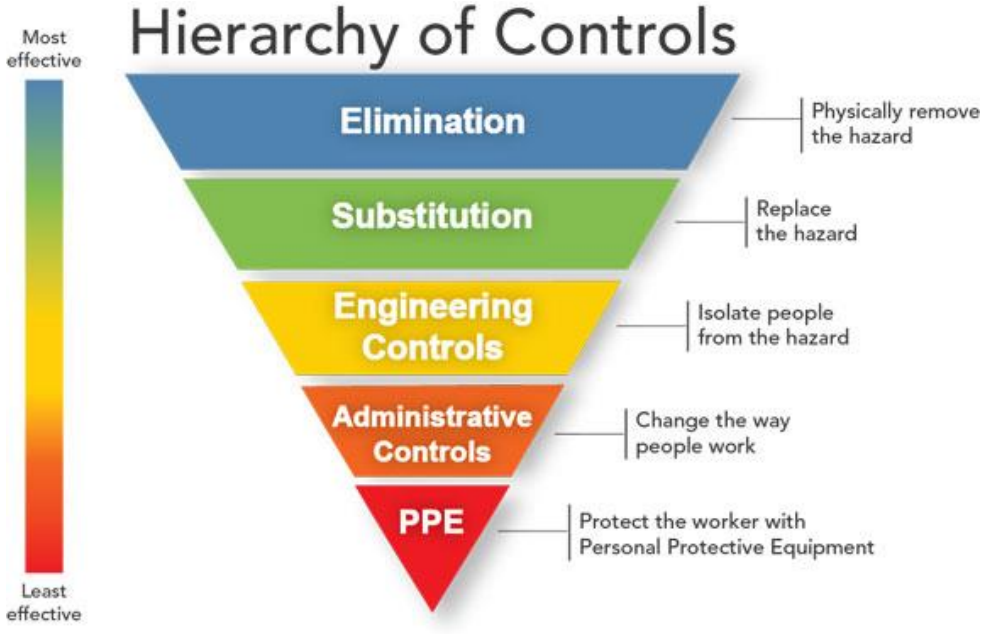
Risk treatment involves selecting one or more options for modifying a risk by changing the consequences that could occur or their likelihood and implementing those options. Action is taken to eliminate or reduce the negative impacts or to maximise potential benefits.

Risk treatments may include:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- accepting the risk or taking the risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood of the risk;
- changing the consequences of the risk;
- transferring or sharing the risk in full or in part; and/or
- retention of risk by informed decision.

Where controls exist and are considered effective to manage the risk so that it falls below the ALARP line, no further action is required except for periodic monitoring. Where existing controls fail to manage the risk to below the ALARP line, risk management plans should be developed and implemented to mitigate the risks to an acceptable level.

Elimination must be considered as the preferred treatment for risks. Where it isn't reasonable or practicable to eliminate the risk, control measures need to be implemented to reduce it to the lowest level possible. The hierarchy of controls is a list of control measures, in priority order, that can be used to eliminate or mitigate the risk.



Examples of generic risk controls which can reduce or transfer the risk include:

- documentation and implementation of plans, policies and procedures;
- segregation or separation of duties;
- authorisation or review of transactions or decisions;
- retention and protection of records;
- supervision or monitoring of operations;
- trend identification and review;
- delegations of authority;
- maintenance programs;
- management reviews;
- independent internal/external reviews;
- contingency plans;
- IT security;
- controls over information processing;
- training and communication;
- performance management/appraisal;
- staff rotation;
- expert advice/referrals;
- physical safeguards; and/or
- insurance policies.

Controls can be categorised as preventive, detective or corrective. Preventive controls tend to be proactive in that they are designed to keep errors or irregularities from occurring in the first place. Detective and corrective controls tend to be reactive, being implemented if the risk event occurs and acting to limit the damage. Examples of preventive, detective and corrective controls include:

Preventive	Detective	Corrective
segregation of duties	petty cash audits	IT back ups
policies & procedures	bank reconciliation	
training	stocktakes	changes to IT access if role changes
position descriptions	Internal audit	
passwords	reviews	Disaster Recovery Plans
authorisation signatures		

Sample preventive, detective and corrective controls

Some controls are effective to reduce the likelihood of a risk event occurring while others are effective to reduce the consequence. For example, internal process controls can reduce the likelihood while an insurance policy can reduce the consequences.

As the residual risk level considers the likelihood and consequence of a risk occurring in light of existing controls, Council's risk register will document the effectiveness of each identified control as detailed below.

Effective	Control is effective in most circumstances; will have a significant effect in terms of reducing the likelihood and/or consequence; provides assurance that this risk will not occur
Somewhat effective	Control is partially effective most of the time; will have some effect in terms of reducing the likelihood and/or consequence; some weaknesses/inefficiencies have been identified; improvements are required
Ineffective	Control is not effective; will not have any effect in terms of reducing the likelihood and/or consequence; little or no assurance that risk will not occur, many weaknesses/ inefficiencies exist

Control effectiveness

As risk treatments are only effective if they are completed, all risk treatments must be adequately resourced and allocated to a responsible officer for implementation.

The risk register must be updated to reflect completion of the treatment and the risk must be reassessed as to whether these actions have been successful in reducing the likelihood and/or consequence.

Where a decision is taken to accept a risk, the risk is still to be recorded in the risk register along with the reasons behind the decision not to treat the risk.

Monitoring and Review

Monitoring of the risk management system will align with Council's business improvement approach and have the flexibility to adapt to the changing needs of the organisation. Compliance with the Risk Management Policy and the growth in maturity of our risk management system will be monitored by Manex.

As few risks remain static, they need to be regularly reviewed to ensure that the identified risk and associated treatments remain relevant and that changing circumstances don't alter priorities or expected outcomes.

Risk Owners are to monitor the accuracy, currency and status of the risks that have been allocated to them and report on them in accordance with the requirements of this plan. This monitoring is to include obtaining assurance that the controls associated with the risk are effective.

All risk registers will be formally reviewed on a six (6) monthly basis. One of these reviews should coincide with the annual integrated planning and budgeting process. This helps determine work priorities and ensures appropriate resources are assigned to manage and control risks. Each risk register needs to be robust to ensure that the risk controls listed can be cross-referenced to Council's document management system and/or document convention.

Council's risk management framework, policies and practices will be reviewed at least once every two (2) years. This review should assess:

- the adequacy of risk management policies and procedures
- compliance with risk management policies and procedures
- the effectiveness of policies, procedures and controls in mitigating risks.

The review may be included in the internal audit program but may also be conducted outside this process or through an alternative process that examines these aspects of risk management (e.g. Office of Local Government review, general review of governance).

Definitions

The following terms, as defined in AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines, will apply:

Consequences	Outcome of an event affecting objectives. (AS/NZS ISO 31000:2009)
Control	Measure that is modifying risk. (AS/NZS ISO 31000:2009)
Exposure	The risk exposure is a qualitative value of the sum of the consequences of an event multiplied by the probability of that event occurring.
Likelihood	Chance of something happening. (AS/NZS ISO 31000:2009).
Residual Risk	Risk remaining after risk treatment. (AS/NZS ISO 31000:2009)
Risk	Effect of uncertainty on objectives. (AS/NZS ISO 31000:2009)
Issue/Incident	An event that has occurred that has taken Council outside its target level of risk.
Risk Acceptance	An informed decision to accept the consequences and the likelihood of a particular risk.
Risk Analysis	A process to comprehend the nature of risk and to determine the level of risk. (AS/NZS ISO 31000:2009)
Risk Avoidance	An informed decision to withdraw from, or to not become involved in, a risk situation.
Risk Identification	Process of finding, recognizing and describing risks. (AS/NZS ISO 31000:2009)
Risk Register	A Risk Register provides a repository for recording each risk and its attributes, evaluation and treatments.
Risk Source	Element which, alone or in combination, has the intrinsic potential to give rise to risk. (AS/NZS ISO 31000:2009)
Risk Management	Coordinated activities to direct and control an organisation with regard to risk. *(AS/NZS ISO 31000:2009)*

Risk Management Plan	Scheme within a Risk Management Framework specifying the approach, the management components and resources to be applied to the management of risk coordinated activities to direct and control and organization with regard to risk. (AS/NZS ISO 31000:2009)
Risk Owner	Person or entity with the accountability and authority to manage a risk. Scheme within a Risk Management Framework specifying the approach, the management components and resources to be applied to the management of risk coordinated activities to direct and control and organization with regard to risk. (AS/NZS ISO 31000:2009)
Risk Retention	Intentionally or unintentionally retaining the responsibility for loss, or financial burden of loss within the organization. Scheme within a Risk Management Framework specifying the approach, the management components and resources to be applied to the management of risk coordinated activities to direct and control and organization with regard to risk. (AS/NZS ISO 31000:2009)
Risk Sharing	Sharing with another party, the burden of loss or benefit of gain, for a risk. (AS/NZS ISO 31000:2009)
Risk Treatment	Process to modify risk (AS/NZS ISO 31000:2009).
Stakeholder	Person or organization that can affect, be affected by, or perceive themselves to be affected by, a decision or activity (AS/NZS ISO 31000:2009).
Target Level of Risk	The highest level of risk for each category that Council is willing to accept without escalating the risk to an authorized person for acceptance.

Authorisation Details

Authorised by:	Council
Minute No:	402
Date:	30.6.20
Review timeframe:	2 years from date of adoption
Department:	Integrated Planning, Risk and Governance
Document Owner:	Manager, Integrated Planning, Risk and Governance
DOC ID:	1133980
Relevant Legislation:	▪ Local Government Act (NSW) 1993 ▪ AS/NZS ISO 31000:2018 Risk Management and Principles Guidelines
Related Policies/Procedures	▪ Enterprise Risk Management Policy

Details History

Version No.	Date changed	Policy type	Modified by	Amendments made
1	N/A	External	Risk and Improvement Officer	First Version