Integrity, Respect, Teamwork, Accountability and Excellence

Cessnock City Council
Enterprise Risk Management Framework

Date Adopted: on: **17 March 2021**

Contents

1. Background and Purpose

Risk

All organisations, including Councils, operate in uncertain and changing economic, social, political, legal, business and local environments. Risk is defined as the effect of this uncertainty on an organizations ability to achieve its goals and objectives, where the effect is the potential for a result that is different to what was expected or planned for.

Risk can be positive, negative or both, and can address, create or result in opportunities or threats.

2. Objectives

To provide an Enterprise Risk Management (ERM) framework that takes a proactive approach in identifying, analyzing, evaluating and treating risks at Cessnock City Council (Council).

Council will seek to meet the principles of risk management as listed in *AS ISO 31000:*2018 Risk *Management* – based on the following eight specific principles to ensure it is effective:

- Risk management is integrated into all organisational activities and decision – making processes
- Risk management is a structured and comprehensive process that achieves consistent and comparable results
- The risk management framework and process is customised to the organisation
- Risk management is inclusive of all stakeholders and enables their knowledge, views and perceptions to be considered
- Risk management is dynamic and able to respond to changes and events in an appropriate and timely manner
- Risk management decisions are based on the best available information and take into account any limitations and uncertainties
- Risk management takes into account human and cultural factors

- Risk management is continuously and periodically evaluated and improved through learning and experience

3. Scope

The purpose of the ERM framework is to establish a consistent and structured approach to risk management with the aim of assisting 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;
- Externally imposed Government changes;
- 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, consultation 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.

4. Statement

4.1. Mandate and Commitment

Council is committed to effectively and systematically managing risks in order to maximise opportunities and limit effects in accordance with *AS ISO 31000:2018 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.

4.2. Roles and Responsibilities

All levels of Council have a responsibility for managing risk, and a role to play in ERM. The specific roles are detailed below.

3.2.1 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.

3.2.2 General Manager

The General Manager is responsible for providing strong leadership and support to fulfill the requirements of the ERM Framework. The General Manager also holds the responsibilities of the Executive Leadership Team.

3.2.3 Executive Leadership Team

The Executive Leadership Team (ELT) is responsible to drive risk management across the organisation and to implement it in their respective areas of accountability in line with *AS ISO 31000:2018 Risk Management* – Principles and guidelines. They are responsible to allocate 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. They will also ensure communication and strong leadership and commitment to risk management.

3.2.4 Managers

Managers are responsible to manage risk in their respective areas of accountability and responsibility and to support employees in identifying, managing and communicating risk. They are responsible for the development, ongoing review and refinement of operational risk registers within their areas of accountability and to escalate risks in accordance with Council's escalation process.

3.2.5 Safety and Risk Team

The Safety and Risk Management team is responsible to develop and maintain risk management frameworks, procedures, tools and training to provide technical risk management support to the organisation. They are responsible for regular reporting to the ELT on risk management activities and facilitating the development, updating and continuous improvement of risk registers across the organisation.

3.2.6 Workers

All Workers are responsible for embracing, promoting and maintaining Council's risk management practices within their particular area of responsibility. Employees are also required to ensure implementation of the Enterprise Risk Management Framework in all areas of the business.

3.2.7 Audit and Risk Committee

The Audit and Risk Committee is responsible for reviewing Council's Enterprise Risk Management Framework on a annual basis, or as required, to ensure compliance with relevant risk management standards and provide continual improvement guidance based on risk management performance measures. The Audit and Risk Committee is also required to review strategic and operational risk assessments to ensure Council management have adequate controls in place and the framework is implemented into all areas of Council business.

3.2.8 Internal Auditor

The Internal Auditor is responsible for implementing an internal audit program to ensure compliance against Council's Enterprise Risk Management Framework and provide regular reports to the General Manager and Audit and Risk Committee on the organisations risk management performance as required by the Local Government Act 1993.

3.3 Risk Management Process

3.3.1 General

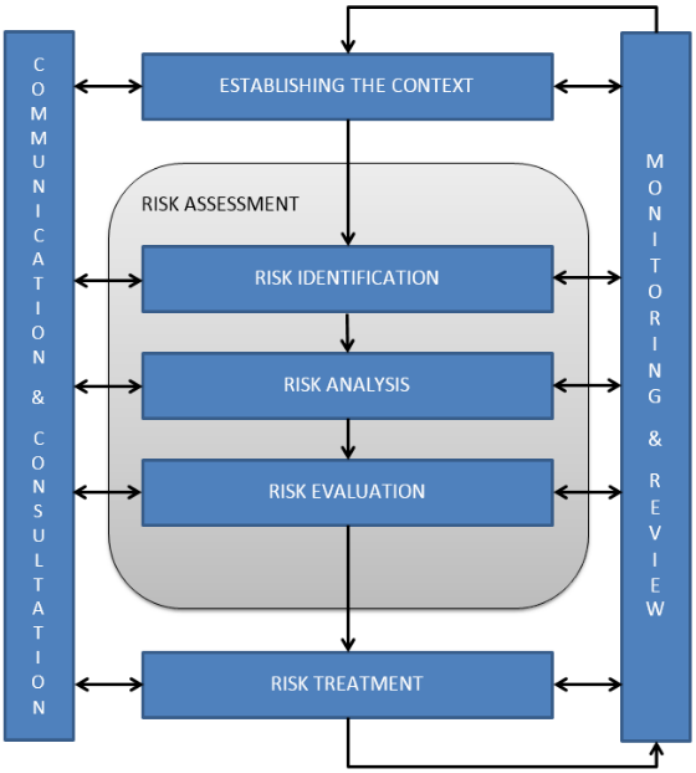
Risk management describes the coordinated activities an organisation takes to ensure it knows the risks it faces, makes informed decisions about how to respond to these risks and identifies and harnesses potential opportunities. In practice, it is a deliberate, systematic, comprehensive and documented approach that provides a structure to managing risk consistently across the entire organisation. It will provide a mechanism to shape organisational culture and promote good business practices.

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.

3.3.2 Risk integration

Integration of risk should be dynamic and iterative process, customised to Council's unique needs and culture. Risk management must be part of Council's purpose, governance, leadership, strategy, objectives and operations and everyone must understand their role in managing risk.

The risk management process is illustrated below.



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.

3.3.3 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 enterprise 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 and Risk Committee and give due consideration to risk management issues raised in Council reports.
- **Audit and Risk Committee –** The Audit and Risk Committee will review Council's ERM Framework, Strategic Risk Register and business continuity management arrangement to ensure the adequacy of our processes for managing risks.
- **Executive Leadership Team –** The ELT will prepare the Strategic and Corporate Risk Register on a regular basis. Emerging and changing risks will be identified and added to the relevant risk register. The ELT will also review key risk management metrics on a monthly basis. The Safety and Risk team will coordinate risk management information, metrics and business plans required for ELT to effectively oversee the risk management function.

3.3.4 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)
- Social responsibility issues;
- The threats and opportunities faced by Council;
- The Local Government Act and other legislation of key relevance;
- The physical environment Council operates within; 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 under the internal context include:

- Goals and objectives and the strategies that are in place to achieve them;
- Organisational culture;
- Strategic drivers;
- Organisation structure;
- Risk culture – including risk appetite and risk tolerance;
- The strengths and weaknesses of Council;
- Internal stakeholders e.g volunteers, contractors; and
- Organisational resources such as people, systems and processes.

The risk management context is the level of detail that will be entered into during the risk management process prior to commencement. The extent and scope of the risk management process will depend on the goals and objectives of the council activity which is likely to inform the budget, scope and importance that has been allocated. In each instance, consideration must also be given to the roles and responsibilities from implementing and the undertaking of the risk management process.

3.3.4 Risk Categories

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. The risk categories will be applied to sort risks as a basis for comparison, reporting and decision making.

Risk Category	Definition (Examples)
People	Injury/illness to employees, contractors, members of the community and any other person.
Environmental	Damage to or pollution of land, water, air, flora and fauna.
Assets	Damage, theft, failures and maintenance of Council assets.
Compliance	Compliance with applicable laws, industry codes, standards etc.
Financial	Sustainability, revenue, grants, expenditure.

Reputation	Public perception and opinion.
Operations	Human Resources, service delivery and Council operations.
Technology & Systems	Information management and systems of work.

3.3.5 Target Level of Risk

Council accepts that there is risk in all operations and functions and that the target level of risk will vary depending on the category of risk. Council recognises that in some instances it will have a higher target level of 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 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 target level for risks that may foreseeably:

- Compromise the health, safety and wellbeing of people whether they be workers 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 section 3.3.8.

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

It is impractical for Council to adopt a target level of 'low' for all impact areas as this would create a significant resource burden in attempting to reduce all risks to 'low' and an administrative burden to escalate all risk above that level. Where existing control measures do not minimise risks to the stated target level or below, the risks will be escalated and assigned to the appropriate level of authority within Council. The table below identifies those with the authority for the acceptance of these risks:

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

3.3.6 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 31000:2018*, 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.

3.3.7 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 (LTI)	Significant injury or long term illness; hospitalisation	Fatality; Permanent disability, illness or disease.
Environmental	Little or no environmental harm. Isolated and immediately reversible.	Minor environmental impact; isolated & reversible or localised and immediately reversible.	Moderate emvironmental impact; loacalised and reversible or isolated and irreversible.	Significant environmental impact; regional and reversible or localised ad irreversible.	Catastrophic environmental impact; national and reversible or regional and irreversible.
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.
Legal	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 (Whichever is less)	Negligible financial loss or less than $10,000 or up to 10% of program/project value.	Minor financial loss; $10,000 - $50,000 or 10% - 15% of program/project value.	Significant financial loss; $50,000 - $500,000 or 15% - 25% of program/project value.	Major financial loss; $500,000 - $1m or 25% - 50% of program/project value.	Extensive financial loss or 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 or 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**	All of the controls associated with the risk are extremely weak and/or non-existent. Without control improvement there is almost no doubt whatsoever that the risk will eventuate
B	**Likely**	The majority of the controls associated with the risk are weak. Without control improvement it is more likely than not that the risk will eventuate.
C	**Possible**	There are some controls that need improvement, however, if there is no improvement there is no guarantee the risk will eventuate.
D	**Unlikely**	The majority of controls are strong with few control gaps. The strength of this control environment means that it is likely that the risk eventuating would be caused by external factors not known to the organisation.
E	**Rare**	All controls are strong with no control gaps. The strength of this control environment means that, if this risk eventuates, it is most likely as a result of external circumstances outside of our control.

Level of Risk

	Consequence Severity Level				
	1	2	3	4	5
A	Medium	High	High	Extreme	Extreme
B	Medium	Medium	High	High	Extreme
C	Low	Medium	Medium	High	High
D	Low	Low	Medium	Medium	High
E	Low	Low	Medium	Medium	High

Risks can be assessed 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 residual 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.

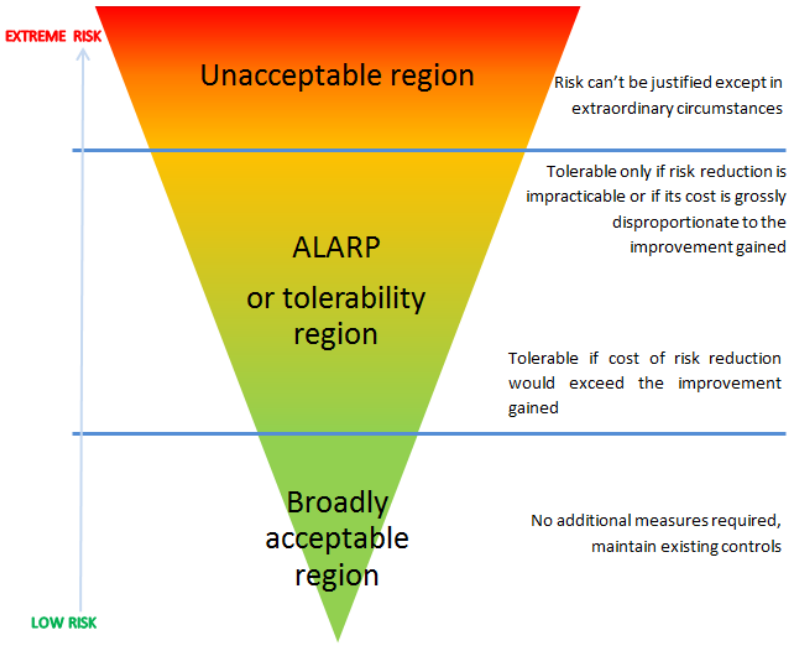
3.3.8 Risk Evaluation

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)



3.3.9 Risk Treatment

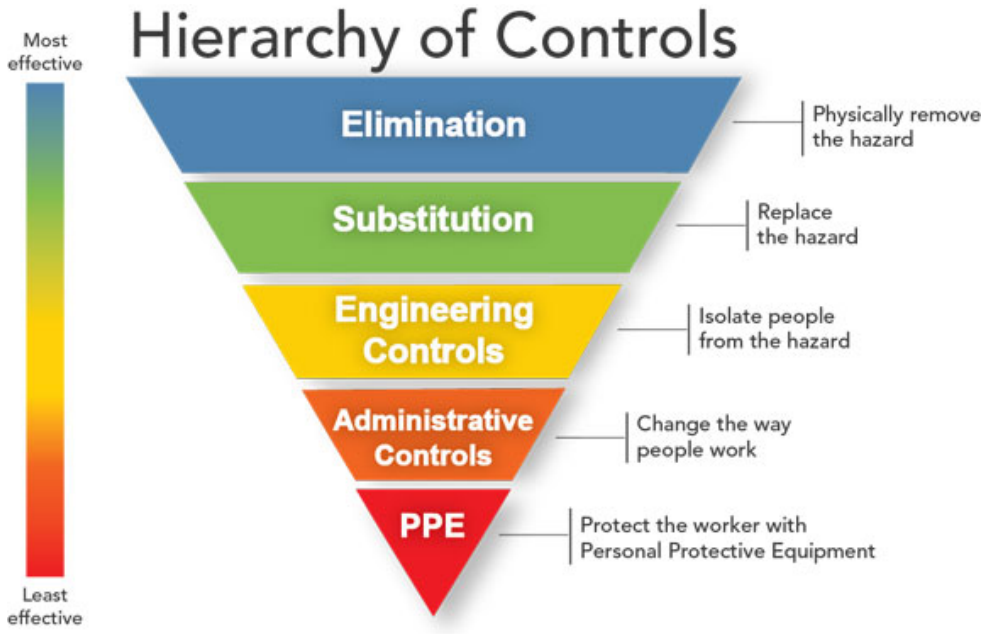
Risk treatment involves selecting one or more options for modifying a risk by changing the consequences that could occur or their likelihood and implementing those options. Action is taken to eliminate or reduce the negative impacts or to maximise potential benefits.

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	Business Continuity Plans
Policies & procedures	Bank reconciliation	
Training	Stocktakes	Changes to IT access if role changes
Position descriptions	Internal audit	
Passwords	Reviews	Disaster Recovery Plans
Authorisation signatures		

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 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.

Control Effectiveness

The following table provides a useful methodology for the assessment of the effectiveness of existing controls:

Not Effective	Not effective at all in mitigating the risk (will not have any effect in terms of reducing the likelihood and/or consequence of the risk)
Negligible	Partial control in some circumstances (will have very little effect in terms of reducing the likelihood and/or consequence of the risk)
Reasonably Effective	Partial control most of the time (will have some effect in terms of reducing the likelihood and/or consequence of the risk)
Mostly Effective	Effective in most circumstances (will have a reasonably significant effect in terms of reducing the likelihood and/or consequence of the risk)
Effective	Fully effective at all times (will significantly reduce the likelihood and/or consequence of the risk at all times).

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.

3.3.10 Monitoring and Reviewing

Monitoring of the enterprise risk 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 the Executive Leadership Team.

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 twelve (12) 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 enterprise riskrisk 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).

4 Definitions

The following terms, as defined in *AS/NZS ISO 31000:2018 Risk Management* – Principles and guidelines, will apply:

Consequences	Outcome of an event affecting objectives (AS/NZS ISO 31000 - 2018).
Control	Measure that is modifying risk (AS/NZS ISO 31000 - 2018).
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 - 2018)
Measure of success	Such measures include costs, reductions impact and/or likelihood and reductions in occurrence.
Residual Risk	Risk remaining after risk treatment (AS/NZS ISO 31000 - 2018)
Risk	Effect of uncertainty on objectives. (AS/NZS ISO 31000 - 2018)
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation.
Issue/Incident	An event that has occurred that has taken Council outside its target level of risk.
Risk appetite	The tolerance of attitude that an organisation or part of (e.g. project) has for risk. How conservative is an organisation
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 - 2018).
Risk Avoidance	An informed decision to withdraw from, or to not become involved in, a risk situation.
Risk Identification	Process of finding, recognising and describing risks (AS/NZS ISO 31000 - 2018)
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 - 2018).
Risk Management	Coordinated activities to direct and control an organisation with regard to risk (AS/NZS ISO 31000 - 2018).
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 an organisation with regard to risk (AS/NZS ISO 31000 - 2018).
Risk Owner	Person or entity with the accountability and authority to manage a risk (AS/NZS ISO 31000 - 2018).
Risk Retention	Intentionally or unintentionally retaining the responsibility for loss, or financial burden of loss within the organization. (AS/NZS 4360:2004)
Risk Sharing	Sharing with another party, the burden of loss or benefit of gain, for a risk. (AS/NZS 4360:2004)
Risk Treatment	Process to modify risk (AS/NZS ISO 31000 - 2018).
Stakeholder	Person or organisation that can affect, be affected by, or perceive themselves to be affected by, a decision or activity. (AS/NZS ISO 31000 - 2018)
Target Level of Risk	The highest level of risk for each category that Council is willing to accept without escalating the risk to an authorised person for acceptance.

5 Administration

Business Group:	General Managers Unit
Responsible Officer:	Human Resource Manager
Review Date:	Two (2) years from date of adoption
File Number / Document Number:	DOC2021/058893
Relevant Legislation:	• Local Government Act (NSW) 1993 • *AS/NZS ISO 31000: 2018* Risk Management – Principles and guidelines
Related Policies / Frameworks / Procedures	• Risk Management Policy

6 History

Revision	Date Approved / Authority	Description of Changes
1	7th March 2018 /	New framework adopted
2	22 November 2019	Changed wording of 'moderate' to 'possible' in the likelihood descriptors. Added the word 'existing' to Target Level of Risk on page 9.
3	17 March 2021	Review