RISK MANAGEMENT PLAN

Wentworth
SHIRE COUNCIL

This document was compiled by Wentworth Shire Council.

Copies of this plan can be viewed online at www.wentworth.nsw.gov.au

Wentworth Shire Council
Risk Management Plan

Index

Introduction

The management of risk, in conjunction with other management directions, is integral to achieving excellent governance and corporate support for delivery of our Strategic Plan and achievement of our strategic goals.

Effective management of risk begins with Council's leadership and the consideration of our operating environment and our appetite for taking risk. We do this with all our decisions but especially when formulating an effective strategy and goals for Council.

A pragmatic approach for managing risk includes the identification, evaluation and implementation of appropriate treatment strategies to manage our risks, and therefore better manage our operations. Risks that would disrupt operations and therefore our strategic goals encompass threats (potential adverse impacts) and opportunities (potential favourable impacts), both of which we must be prepared to identify and manage.

Council recognises risk management as an integral part of better management practice and decision-making. As such, the objectives of this Enterprise Risk Management Plan are to:

- Adhere to the Enterprise Risk Management Policy;
- Provide a framework within which we can sustainably create, preserve and protect the value inherent in our community, our assets and our operations;
- Create an environment where all employees assume responsibility for managing risk;
- Achieve and maintain legislative and regulatory compliance;
- Ensure resources and operational capabilities are identified and responsibly allocated for managing risk;
- Ensure Council can appropriately deal with risk;
- Demonstrate transparent and responsible risk management processes which align with accepted better practices;
- Provide documented evidence of Council's commitment to adopting risk management principles as an integral part of operations and decision-making; and
- Develop and implement the risk management program and make recommendations for continuous improvement of the program.

Purpose

This Plan is a key component of Council's Enterprise Risk Management Framework, which also consists of, the Enterprise Risk Manual, the Enterprise Risk Management Policy, and the Enterprise Risk Management Procedure. This document, the Enterprise Risk Management Plan (ERMP) will be reviewed every (2) years, or as key references are updated. The ERMP will provide an overview of:

- how the various Risk Management Framework components are linked and support each other;
- the key concepts of risk management and why we do it;
- details regarding the recording, reporting and reviewing of risks; and
- guidance to staff in relation to the governance of risk management.

The aim of Council's Enterprise Risk Management activities is to:

- identify Strategic risks that can potentially impact (positively or negatively) on the achievement of Strategic goals;
- identify Operational risks that are inherent in the main functions performed by Council;
- develop and maintain a common Risk Register for Strategic, and Operational risks; and
- establish a culture where individual activities are risk assessed as part of every function performed.

Scope

This document applies to all Councillors, executives, staff, contractors, operations and activities. The management of risk is an essential element of better management practices and impacts on every element of the organisation's activity. As such, the principles and processes of Enterprise Risk Management (ERM) will be applied as standard and normal practice throughout Council's management processes and operations.

The ERMP will apply to, but not be limited to, the following areas of Council activities:

- Administration and Governance
- General and legal compliance
- Infrastructure and Works operations
- Planning, Environment and Regulatory Compliance
- Strategy and Performance
- Human Resources
- Information Communication and Technology systems
- Financial management and procurement
- Project Management
- Contract Management
- Environmental Management
- Disaster and Emergency Planning, and Business Continuity Planning

Council's Enterprise Risk Management Framework has both behavioural and tangible components including a suite of documents that together provide a comprehensive coverage of Council's approach to the management of its risks.

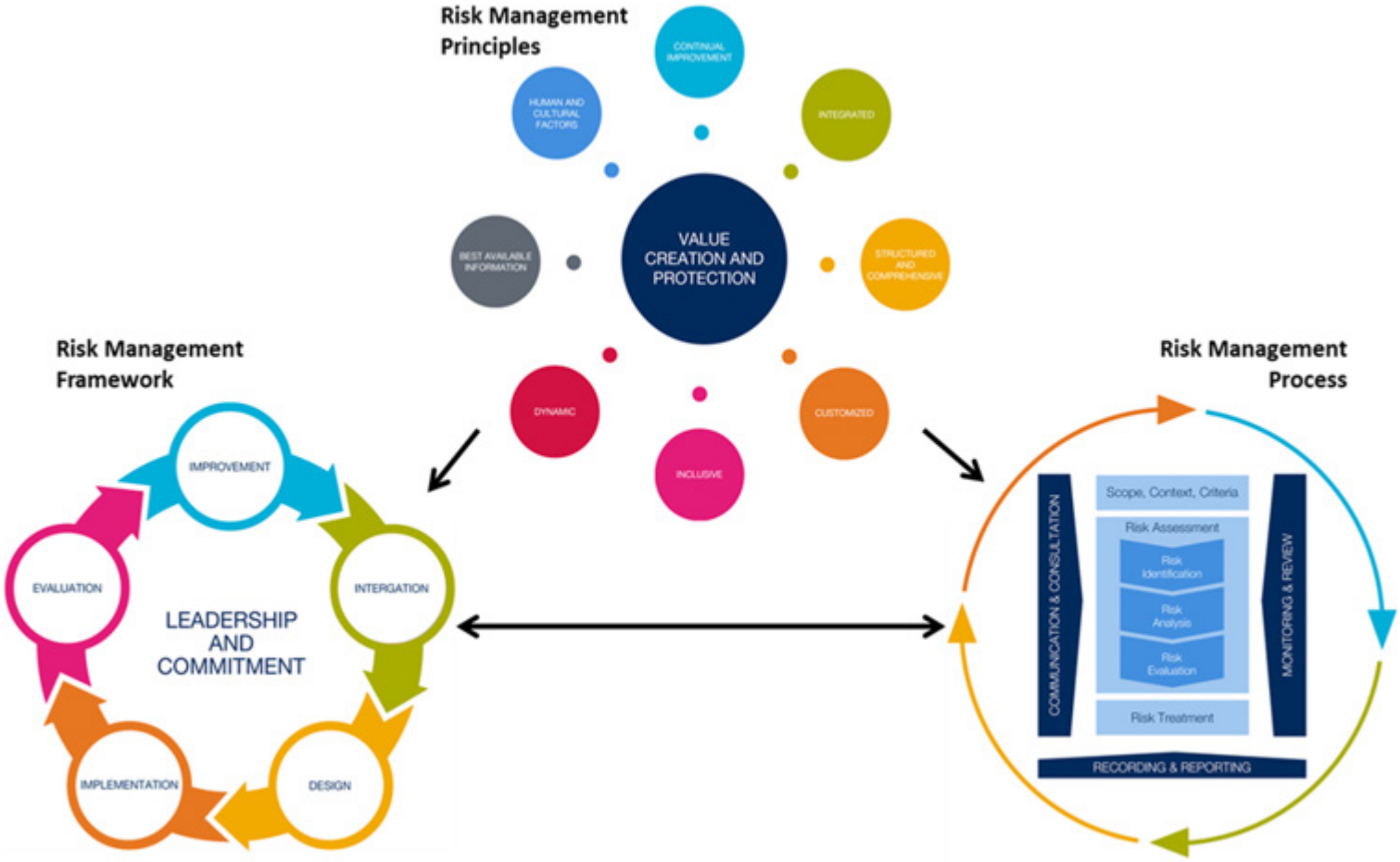
Accountabilities & Responsibilities

Position	Accountabilities
Mayors, Councillors	• In consultation with the Senior Management Team (SMT) and Audit, Risk & Improvement Committee (ARIC) o Endorses Council's appetite for taking and/or retaining risk; o Sets Council's strategy with consideration of the risk appetite and the threats and opportunities to Council from that strategy; o Set the strategic goals required to achieve the strategy and clearly articulates the critical success factors in achieving those strategic goals; and o Articulates, the strategic risks (threat and opportunity) to Council from the objectives and strategy. • Requires the SMT to actively manage strategic risks and report frequently on their status. • Recognises their responsibilities for making informed decisions that take into consideration the associated risks and opportunities. • Actively supports the implementation of the ERM Policy and ERMP.
Audit, Risk & Improvement Committee (ARIC)	• Independent review and oversight of Council's governance, risk management and control activities. • Oversight of risk management at Council and the Internal Audit function • Requires the periodic review of Council's strategic and other significant operational risks to ensure appropriate risk treatment/ controls have been implemented and maintain effectiveness.
Internal Audit	• Risk assurance to the ARIC and GM through execution of the annual internal audit plan.
General Manager	• Overall accountability for Council's management of its risks. • Accountable for the establishment of the Enterprise Risk Management system in Council and leads the conversation about risk. • Implementing the tone, culture and expectations for risk management and governance activities, and assigns appropriate responsibilities to the SMT • Ensures adequacy of resources for risk management activities and sets appropriate delegations for risk management activities. • Establishes performance measures for the strategic goals' critical success factors and drives the Council's Enterprise Risk Management objectives.

Position	Accountabilities
Senior Management Team	• Accountable for ownership and management of risks in their respective areas. • Creates an environment where managing risk is an accepted and expected part of the normal operations. • Accountable for the effective implementation and continual improvement of the ERMP. • Implements monitoring and management of relevant performance measures for strategic goal's critical success factors within their area of responsibility. • Ensures that strategic and significant risks are reported in accordance with the ERM reporting requirements. • Recommends recurrent and discretionary allocation of funding for the purpose of managing risks identified as priority in accordance with the ERMP.
Director Finance & Policy	• Leading the risk management function. • Responsible for developing, implementing and managing an Enterprise Risk Management Framework that is fit for purpose. • Responsible for reporting strategic risks and certain residual risks to the Audit, Risk & Improvement Committee. • Supporting the organisation to manage its risks through: o provision of risk management advice and guidance to staff, and o maintenance of the risk management framework.
Department Managers	• Accountable for managing risk within their area of responsibility, including monitoring and managing measures for the strategic goals' critical success factors. • Ensures that employees and relevant stakeholders apply the appropriate risk management tools and templates in the correct manner. • Are responsible for providing assistance and advice to staff in relation to the management of risks but not to take on the responsibility of another individual. • Monitor the respective operational risk profile assessments, determine and ensure implementation of control measures for risks identified, and escalate any significant risks to management in accordance with the risk management protocols. • Responsible Contract/Project Managers are to ensure risks associated with the engagement of contractors are appropriately identified and managed. • Responsible Contract/Project Managers are to ensure the responsibilities and accountabilities vested in the contractor are clearly documented and communicated to the Contractor.
All Staff & Contractors	• Applying sound risk management practices in accordance with Council policies and frameworks.

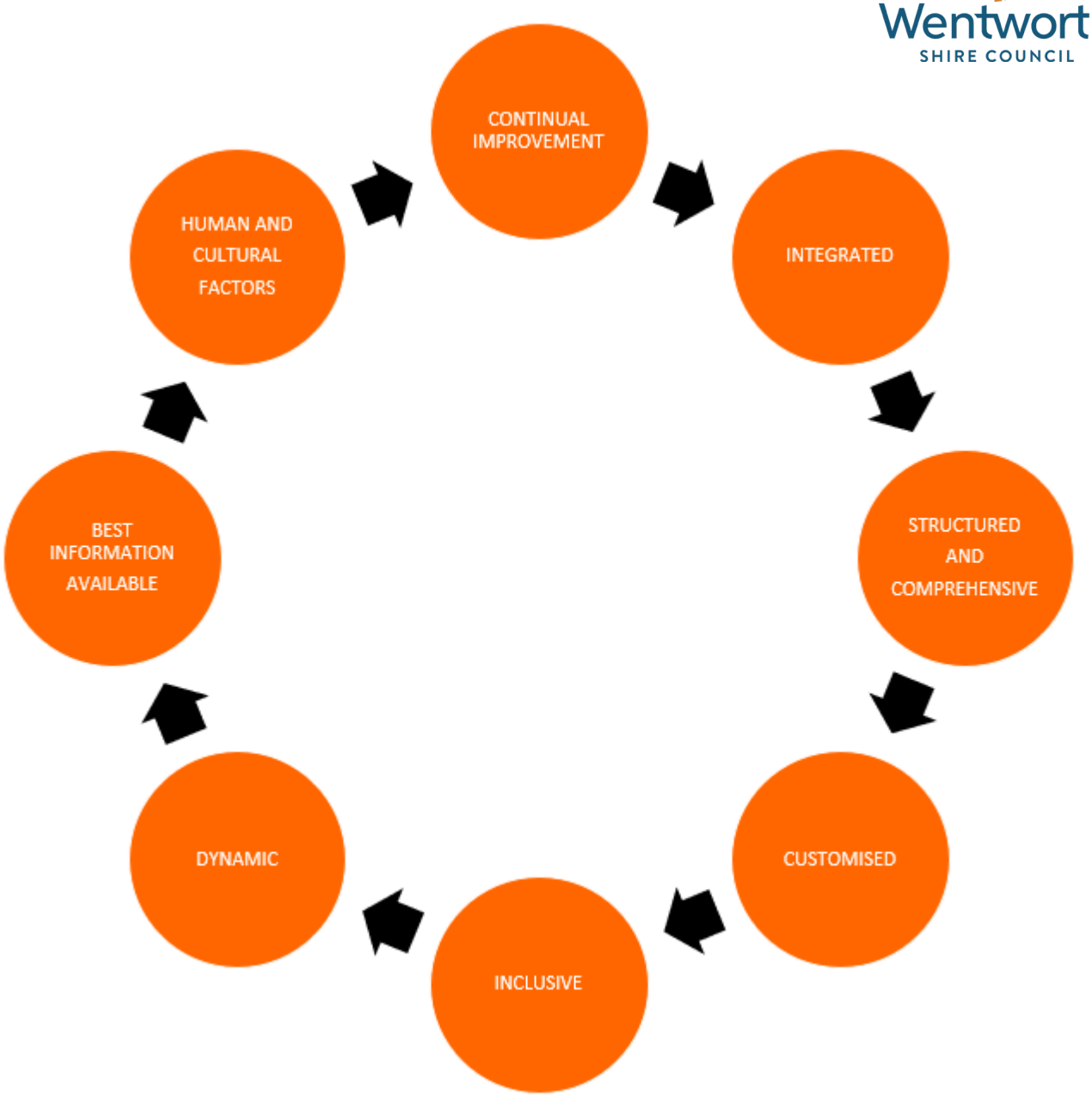
RISK MANAGEMENT PRINCIPLES, FRAMEWORK AND PROCESS

A whole of organisation approach to Enterprise Risk Management is required to effectively and efficiently manage Council's emerging, potential and current risks. To do this the AS ISO 31000:2018 integrated model is used. This model is composed of Framework attributes that are influenced by a set of Principles, and both of which influence a Risk Management Process.



Risk Management Principles

ERM is not a function or a department. It is the culture, capabilities, and practices that organisations integrate with strategy setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realising value. To do this the risk management standard advocates eight principles that provide guidance on the characteristics of effective and efficient risk management activities. These principles are:

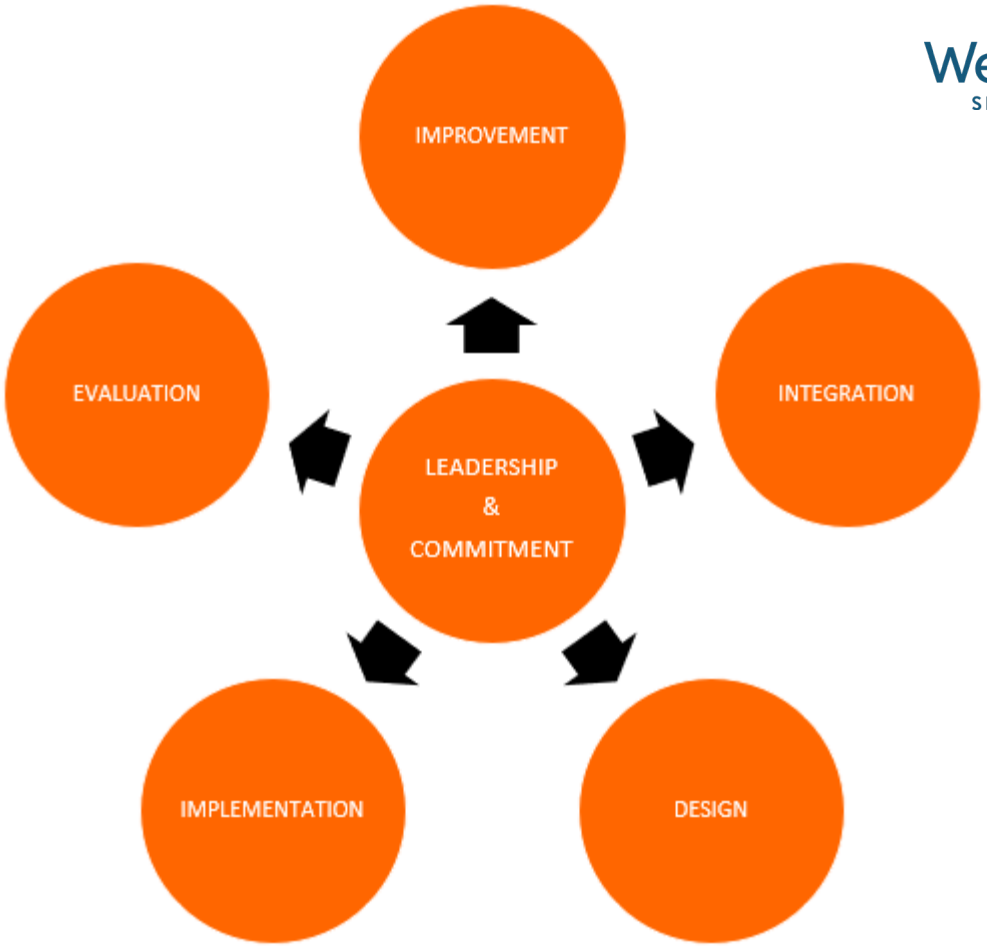


Risk Management Framework

The concept of a risk management framework is to facilitate the integration of risk into significant activities and functions of an organisation. The framework does this by encompassing integration, design, implementation, evaluation and improvement elements into its development, all with explicit commitment from the organisation's leadership.

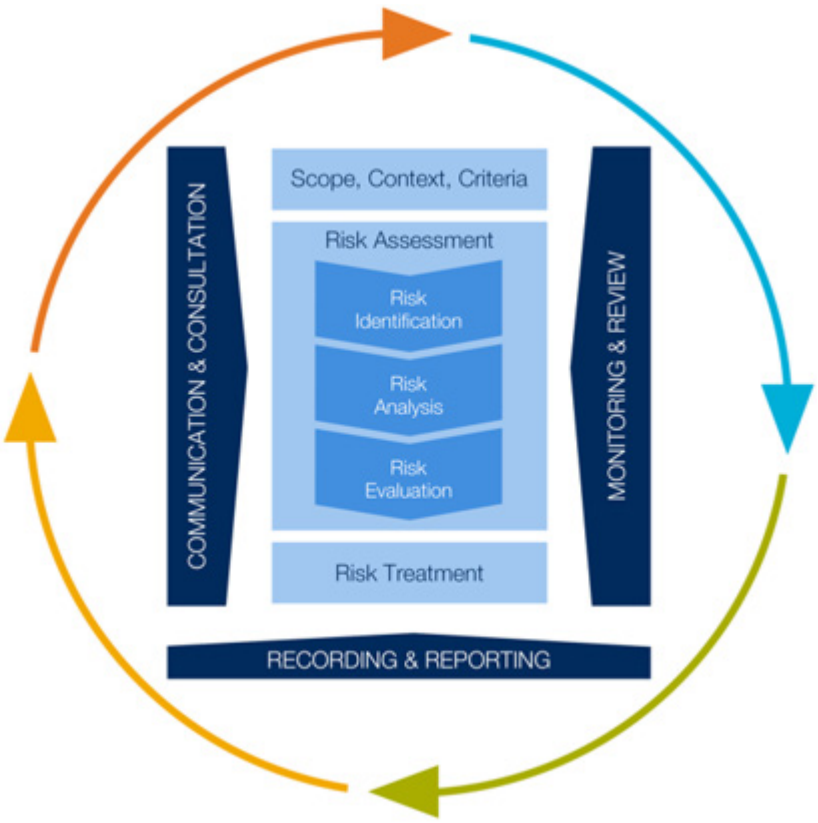
The practical application of these elements creates a risk management framework that consists of tangible documents such as policies, plans, procedures and behavioural aspects such as organisational culture and understood appetites for taking risk.

A key component of the Risk Management Framework is Leadership and Commitment. This component, in the standard specifically states that, *"Top management is accountable for managing risk while oversight bodies are accountable for overseeing risk management."* Further to this statement, the Standard, in defining 'Integration' states, *"Determining risk management accountability and oversight roles within an organisation are integral parts of the organisation's governance."*



Risk Management Process

The risk management process is a structured approach for Council to identify, assess and respond to risk. The process adopted by Council to manage risks follows the process published in the risk management standard. This process can be applied at strategic, operational, program or project levels.



The main elements of the risk management process are defined below.

Communication and Consultation
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.
Scope, Context and Criteria
This part 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.
Risk Identification
This is the first, and arguably most critical, part of the Risk Assessment phase. Risk identification is the process of finding, recognising and recording risks. "*Risk is the effect of uncertainty on objectives"*, it is therefore very important to distil the things that are identified down to only those things that may have a positive or negative impact on reaching organisational objectives. At the risk identification stage, the organisation identifies what, why and how things can arise, that may affect the organisation, as the basis for further analysis. This is done at both strategic and operational levels of the organisation.
Risk Analysis
This is the second part of the Risk Assessment phase and determines various characteristics of the identified risk. This part is where biases, perceptions, judgements and opinions can have a strong influence – so caution should be used. Risk analysis is where the causes, consequences, likelihoods, impacts, controls and levels of risk are identified. Both quantification and qualification methods can be used.
Risk Evaluation
In this final part of Risk Assessment, the evaluation of the analysed risks is used to support decision-making and is usually where the 'Risk Rating' is derived. Evaluation involves comparing estimated levels of risk against the pre-established criteria. This enables risks to be ranked in order to identify the priorities for the management of these risks. The levels of risk achieved will determine if they fall into the acceptable category (LOW) or whether immediate action is required (for example HIGH or EXTREME).
Risk Treatment
Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation. This is an iterative process that involves formulating, planning and implementing a risk treatment, followed by assessing its effectiveness and deciding if any residual risk is acceptable. If the treatment is less effective than desired and/or the residual risk is not acceptable, then further treatment action will be required.

Awareness that a risk treatment can introduce additional risk is also required. There are multiple risk treatment options to select from, including: • Avoid the risk by deciding not to start or continue an activity. • Taking or increasing risk to pursue an opportunity. • Removing the risk source. • Developing or improving controls to change the likelihood or consequence. • Sharing the risk through contracts or insurance. • Retaining the risk by informed decision.
Monitoring and Review
Monitoring and review transcends all stages of the risk management process. It is integral to continuous improvement and establishes consistent review of the performance of the risk management system and outcomes from risk management activity. This stage is the most effective at flagging changes that might affect risk management performance or changes that facilitate new risks that will require assessment.
Recording and Reporting
The risk management process and its outcomes should be recorded and reported through appropriate mechanisms and governance structures of the organisation. This will ensure effective transparency of the risk management function, aid in decision-making of the organisation's leadership and facilitate interaction with stakeholders.

Risk Analysis and Evaluation Criteria

For ease of evaluation, risks are grouped into categories. Any given risk may belong in one or more categories, however based on the context in which it is identified it should be grouped into whichever category is most suitable. The risk categories are also used to differentiate risks when assessing consequence.

Council's risk categories are:

- Reputational
- Financial
- Natural & Environmental
- Security & Operational
- Legal, Regulatory & Political
- People

To effectively undertake risk analysis and risk evaluation, a set of criteria are required to ensure that all risks are assessed with the same tools and in the same way. The criteria for these two critical aspects of the risk management process are manifested as tables for assessing likelihood (probability) and consequence (impact), and through the use of a matrix that will provide a risk rating or level for a given risk. Additionally, processes for escalation of risks provide the required communication aspects for the next phase – Risk Treatment.

Consequence and Likelihood tables

Consequence and Likelihood can be determined against set criteria known as 'descriptors', which provide a five level nominal scale for each risk category. Whilst likelihood descriptors are static across categories, the consequence descriptors can vary based on the category of risk being analysed. The Table below, is the Consequence Table for Council and provides descriptors at each level of consequence for each risk category.

Reputational Risk

Insignificant	Minor	Medium	High	Extreme
• Minor damage to brand, image or reputation	• Some short term negative media coverage. • Local community concern or criticism.	• Significant short term damage to reputation. • Sustained/ prominent local media coverage.	• Sustained damage to image/ reputation. • Adverse national/local media coverage.	• Long term damage to image/ reputation. • Sustained negative media attention.

Financial Risk

Insignificant	Minor	Medium	High	Extreme
• Negligible financial loss < $10k or < 2.5% budget variation. • No impact on program or business operation.	• Minor financial loss $10k - $50k or > 2.5% and < 10% budget variation. • Minimal impact on program or business operation.	• Significant financial loss $50K - $500K or > 10% and < 20% budget variation. • Considerable impact on program or business operation.	• Major financial loss $500K - $1M loss or > 20% and < 50% budget variation. • Severe impact on program or business operation.	• Extensive financial loss > $1M or > 50% budget variation. • Loss of program, or business operation.

Natural & Environmental Risk

Insignificant	Minor	Medium	High	Extreme
• Minimal physical or environmental impact. • Isolated release, controlled through normal operations.	• Minor physical or environmental impact. • Onsite release immediately controlled with local resource.	• Significant physical or environmental impact. • Onsite release contained with assistance of external resources.	• Major physical or environmental impact spreading off-site. • Impact contained using external resources.	• Extensive physical or environmental impact, spreading off-site. • Impact contained using external resources. • Long term remediation required

Security & Operational Risk

Insignificant	Minor	Medium	High	Extreme
• Negligible impact on service delivery. • Resolved through normal operations.	• Short term loss, compromise or interuption of core activities with potential for long-term disruption for non-core activities. • Mostly resolved through normal operations.	• Major loss, compromise or interruption to core activities resulting in medium-term impact on operations. • Resolved with assistance of external resources.	• Critical loss or event requiring replacement of property or infrastructure. • Significant impact on core operations.	• Disaster resulting in destruction or long-term unavilability of infrastructurem systems and resources directly impacting operations. • Significant long-term disruption to core operations.

Regulatory, Legal & Political Risk

Insignificant	Minor	Medium	High	Extreme
• Isolated non-compliance or breach. • Minimal impact resolved through normal operations.	• Minor non-compliance or breach resulting in short term impact on operations.	• Serious breach involving statutory authority or investigation. • Adverse publicity at a local level.	• Major breach with fines and/or litigation. • Widespread adverse publicity.	• Extensive breach resulting in large fines and a possible class action. • Significant threat to the viability of the organisation.

People Risk

Insignificant	Minor	Medium	High	Extreme
• Incident resulting in minor injury • Negligible skills or knowledge loss.	• Minor medical treatment with potential for lost time. • Some loss of staff members with acceptable loss. deficit in skills.	• Significant injury involving medical treatment or hospitalisation and lost time. • Short term loss of skills, knowledge and expertise.	• Serious injury or fatality. • Loss of some key staff resulting in skills knowledge and expertise deficit.	• Extensive long term or multiple fatalities. • Loss of a significant number of key staff impacting on skills, knowledge and expertise.

Council has developed the following likelihood table:

Likelihood Table		
Likelihood Level	**Frequency**	**Probability**
Almost Certain	Expected to occur in most circumstances	61 – 99% of the time
Likely	Probably will occur in most circumstances	41 – 60% of the time
Possible	Might happen at some time	21 – 40% of the time
Unlikely	Could happen, but unlikely	11 – 20% of the time
Rare	Has never occurred before	0 – 10% of the time

Risk Matrix

Once the likelihood and consequence of any given risk has been analysed the risk itself will need to be prioritised for further mitigating action or ongoing monitoring. In order to enable the best use of resources risks are rated as Low, Medium, High or Extreme through the mapping of likelihood and consequence values on a risk matrix. The structure of the matrix provides a rating for the given risk. Council has developed the following risk matrix:

	CONSEQUENCE				
Likelihood	**Insignificant**	**Minor**	**Medium**	**High**	**Extreme**
Almost Certain	**Medium**	**High**	**High**	**Extreme**	**Extreme**
Likely	**Medium**	**Medium**	**High**	**High**	**Extreme**
Possible	**Low**	**Medium**	**Medium**	**High**	**High**
Unlikely	**Low**	**Low**	**Medium**	**Medium**	**High**
Rare	**Low**	**Low**	**Low**	**Medium**	**Medium**

Actions required for different risk ratings

Risk Level	Action Required	Monitoring Level
Extreme	• This risk level requires immediate actions for mitigation • **Risk Owner** to develop specific Treatment Plans for immediate implementation to address both likelihood and consequence levels of the risk • **Risk Owner** to create a Risk Exception Report and send immediately to the Senior Management Team via regular management channels • **SMT** to allocate actions and budget for implementation within one month of notification • Include in normal Risk Profile Reports	• Regular agenda item for Audit, Risk & Improvement Committee • Regular agenda item for Senior Management Team • Daily monitoring of controls and treatments by the Risk Owner

Risk Level	Action Required	Monitoring Level
High	• **Risk Owner** to develop and implement a specific Treatment Plan for high risks • **SMT** to allocate actions and budget to minimise risk for High Risks over 2 months old • **Risk Owner** to report to Senior Management within one month • Include in normal Risk Profile Reports	• Regular agenda item for Audit, Risk & Improvement Committee for High Risks over 3 months old. • Regular agenda item for Senior Management Team for High Risks over 2 months old • Weekly monitoring of controls and treatments by Risk Owner
Medium	• **Risk Owner** to develop and implement a specific Treatment Plan for Medium risks that are above their Target rating • **Risk Owner** to report to Senior Management within the quarter for Medium Risks that are above their Target Rating • **Senior Manager** to allocate actions and budget to minimise risk where existing controls deemed inadequate and monitor Treatment Plan implementation • Include in normal Risk Profile Reports.	• Senior Management to receive quarterly Risk Profile Report that highlights Medium Risks that exceed their Target Rating • Weekly monitoring of controls by Risk Owner
Low	• **Risk Owner** to monitor low rated risks and test controls periodically • **Risk Owner** to ensure the risk and controls are managed via routine procedures where possible • Include in normal Risk Profile Reports	• Weekly monitoring of controls by Risk Owner

Risk recording, review and reporting

Effective management of risk within any organisation depends on good communication and the effectiveness of its reporting mechanisms, recording processes, risk review protocols.

Risk Recording

Risks are recorded after a risk assessment process has been undertaken. All Council risks are to be recorded in the **Master Risk Register** by the designated delegate.

All projects are to have their own separate risk register, however they should also be included in the relevant departmental register in the Master Risk Register. In doing this, at any given time, the entire Risk Profile of Council is available in one document. In addition to their separate risk registers, each project should also have an assessed risk within the Master Risk Register that covers the risk of project failure, risk of non-completion, and any risks that the project's completion will introduce to Council.

Master Risk Register

To effectively understand all the risks that Council has (the Risk Profile), it is imperative that an accurate, up to date and relevant register of risks is kept. This is the Master Risk Register, which in order to maintain its integrity must only be updated by the designated delegate.
However, the Register must also be visible to all Senior Management and Risk Owners.

When to enter a risk in the Master Risk Register

When a staff member identifies a risk, whether through a risk workshop, Toolbox meeting, an incident, or any other method they should notify the risk owner and ensure that they have the following information before contacting the designated delegate:

- A description of the risk;
- How might it disrupt Council Goals, Department Goals or Projects;
- What are the potential causes of the risk;
- What are the potential impacts from a risk event;
- Any factors that might mitigate or control the risk; and
- Who should own the risk

The designated delegate will then liaise with the appropriate staff to analyse, evaluate and record the risk in the Master Risk Register. If the risk is given a residual rating of High, it is immediately reported to the SMT, via their management line.

Risk Review

Quick Review

Risk Owners should conduct a 'quick review' of their risks on a monthly basis and report any required changes to the designated delegate for recording in the Master Risk Register. The 'quick review' is a reminder exercise, which includes:

- familiarising what risks the Risk Owner has;
- what the ratings of these risks are;
- what risks are on increased reporting:
  - Extreme risks
  - High risks that are over 2 months old
  - Medium risks that have exceeded their Target Risk Ratings
  - Risks that have recently changed rating by more than one risk level,
- which controls require closer monitoring.

Semi Annual Review

All risks are to be fully reviewed on a 6 monthly basis jointly by the Risk Owner and the Designated Delegate. These reviews will be scheduled by the Designated Delegate and are mandatory. The reviews will include:

- a review of each element of the risk recorded in the Master Risk Register;
- consideration of whether the circumstances surrounding the risk have changed;
- consideration of whether the operating environment has changed; and
- consideration of whether the risk still belongs in the Master Risk Register.

At the end of the review the staff undertaking it should feel satisfied that the risk is as up to date and accurate as it can be.

Risk Reporting

All risks need to be reported on a periodic basis to ensure that they are understood and being effectively managed. The table below, provides details of the risk reporting regime that is required at Council.

Risk Report	Purpose	Prepared By	Prepared For	Frequency
Risk Profile Report	Provides a snapshot of the Council's Risk Profile including a dashboard and rationale for actions and trends	Designated delegate	Senior Management Team	Monthly
Risk Exception Report	Provides information on risks recently rated as Extreme, High risks that have been High for greater than 3 months, or any risk that has recently changed rating by more than 1 risk level A Risk Exception *Report Template is at Appendix D*	Risk Owner	Senior Management Team	As required
Extreme Risk Report	Part of the Risk Profile reporting for the Audit, Risk & Improvement Committee, and it includes all risks rated High (for longer than 3 months) and Extreme	Senior Management Team	Audit, Risk & Improvement Committee	Quarterly
Key Risk Indicator Report	Provides a dashboard of risk indicators which help understanding of some risk profiles and enhance decision-making capability	Designated delegate	Senior Management Team & Audit, Risk & Improvement Committee	Quarterly

Implementing the Enterprise Risk Management Plan

This Enterprise Risk Management Plan (ERMP), as a key component of the Enterprise Risk Management Framework (ERMF), provides the 'What' of risk management for Council – meaning that it describes what Council will do to manage its risks. However, to be an effective ERMF tool it must first be implemented to ensure that staff understand what Council does to management risk. To ensure that the Plan (and the broader ERMF) is implemented, Council will do the following:

- Provide annual Fundamental Risk Management Training for all Relevant staff;
- Provide periodic presentations on the ERMF; and
- Provide a Communications Plan for the initial implementation and ongoing implementation of the ERMP.

Risk Management Training

It is imperative that staff at the Council understand risk management and how it can be an effective tool for improving efficiency and avoiding foreseeable issues. As such, it is required that all staff at Supervisor level and above undergo annual face-to-face risk management training. Completion of this training should be a key component of staff annual professional development plans.
The training will cover the fundamental aspects of ERM and the risk management process, with a deeper level demonstration of simple analytical techniques.

Periodic Presentation on the ERMF

The ERMF presentations are an important reminder of both the tangible and behavioural aspects of the ERMF, especially the role that organisational culture plays in the development of risk management maturity.

To be effective all documents that advocate certain actions and positions need to be read and understood by those people with responsibilities and accountabilities associated with the document/s.

Key Risk Indicators

Key Risk Indicators (KRI's) will be used to measure the performance of the organisations risk management activities and in the monitoring of risk exposures.

The KRI's will be reported to SMT (at least on a quarterly basis) in assisting Council to maximise Enterprise Risk Management outcomes.

a. Integrity risk culture – number of fraud & corruption activities and the number of integrity related disciplinary matters handled and reported.
b. The number and % of major (Extreme and High) level of risks having had further treatment and the level of risk having been reduced to a lower residual level of risk.
c. The number and % of operational service areas involved in the Enterprise Risk Management process.
d. The number of insurance claims submitted to Council – and the areas to which the claims relate to.
e. The number and $ value of insurance claims paid by Council – and the areas to which the claims relate to.
f. The number and % of staff trained/educated in Enterprise Risk Management related topics – includes annual risk management training.
g. The risk maturity level of Council – level of awareness and understanding throughout the organisation of the Enterprise Risk Management Framework, Policy and associated processes and procedures. Normally to be undertaken bi-annually.

Continuous Improvement Review

As part of efforts to maintain a continuous improvement cycle, this plan will be reviewed every two (2) years by the SMT and reported to the Audit, Risk and Improvement Committee to ensure that it continues to meet the requirements and its intent.

Review of this Plan and the broader Enterprise Risk Management Program may be conducted by using any or a combination of the following:

- Obtaining feedback from Managers/ supervisors;
- Surveying staff at all levels;
- Conducting random interviews of sections of Council;
- The engagement of a consultant to conduct an external review and provide recommendations for a way forward. This may be done after 12-18mths or later into the implementation process or when Council considers it would be useful to do so.

Other reviews should be conducted prior to the scheduled formal review if the need warrants it.

Document Approval

This document is the latest version of this document as approved by the Wentworth Shire Council on the 14/12/2022. All previous versions of this document are null and void.

This document may be amended or revoked by the Council at any time.

Signed..... 27 FEB 2023

General Manager Wentworth Shire Council **Date**

Appendix A - Risk Management Principles

Integrated
To be truly effective the management of risks should be a standardised and integrated component of day-to-day activities in the organisation.

Structured and comprehensive
An effective organisation will have a structured approach in the pursuit of its strategy and strategic objectives. ERM should be an integrated component of this structure, which will, if comprehensive enough, contribute to consistent and comparable results.

Customised
Understand the organisation's operating environment, inside and out. The risk management framework and process are customised and proportionate to the organisation's external and internal context related to its objectives.

Inclusive
Multiple relevant perspectives regarding risks and their management is a very effective method of combating the various inherent human biases. Therefore, appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

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.

Best available information
The inputs to risk management can come from a variety of sources with varying levels of accuracy and relevance, and are based on historical and current information, as well as on anticipation of future outcomes. Effective risk management explicitly takes into account the timeliness, any biases, limitations and uncertainties associated with such information. Additionally, an acknowledgement of information that is not known or complete is necessary.

Human and cultural factors
Human behaviour and culture significantly influence all aspects of risk management at each level and stage. As such, awareness of human biases and an understanding of the desired culture is important at all organisational levels. The organisation defines the desired behaviours that characterise its desired culture, not the environment it operates in.

Continual improvement
Risk management is continually improved through learning and experience. The organisation should pursue this as standard operating procedure.

Appendix B - Risk Management Framework Elements

Leadership and Commitment
Top management and oversight bodies provide explicit commitment to the integration of risk management into all activities of the organisation. Top management will be accountable for managing risk and ensuring that the organisation's risk profile is within acceptable limits. Whereas the oversight bodies are accountable for risk management as a function of the organisation and will set risk-aware strategic objectives and determine the acceptable limits for the risk profile.
Integration
Integrating risk management into an organisation is a dynamic and iterative process, and should be customised to the organisation's needs and culture. Risk management should be a part of, and not separate from, the organisational purpose, core values, governance, leadership and commitment, strategy, objectives and operations.
Design
This facet represents the opportunity for the organisation to embed elements of its culture and core values into the framework and make the framework relevant for all stakeholders. In designing the framework, with a thorough understanding of the organisation's internal and external operating environment (context), the organisation should clearly articulate its commitment to risk management. It can assign responsibilities, roles, authorities and accountabilities, and then make the risk management framework relevant to staff by allocating dedicated or delegated resources to fulfil these responsibilities, and establish appropriate communication and consultation protocols.
Implementation
The allocation of appropriate resources is the key element to successful implementation of an effective enterprise risk management function in the organisation. Successful implementation requires the engagement of stakeholders to enable the organisation to explicitly address uncertainty in decision-making and strategy formulation.
Evaluation
Like all other aspects of the organisation the risk management framework should not be developed or exist in isolation. It must be periodically tested against its purpose, implementation, plans, indicators and expected behaviour, to determine whether it remains suitable in its role of supporting the achievement of organisational objectives.
Risk Treatment
A culture of constant vigilance regarding the quality of risk management and the effectiveness of the framework is essential maintain the required flexibility when unexpected changes occur. Such a culture will also embed a continual improvement mindset within the organisation.

Appendix C - Glossary of Terms

Term	Definition
Consequence	Outcome of a risk event affecting objectives
Enterprise Risk Management	Risk management is the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects that may occur within an organisation. The word 'Enterprise' denotes that the program will include the whole organisation, therefore all risks within all areas of an organisation's operation will be included.
Enterprise Risk Management Framework	A set of components that provide the foundations, framework and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. It will also indicate how risk management will be integrated within/across the organisation.
Enterprise Risk Management Plan	Element of the Risk Management Framework documents - The ERMP details what Council will do to manage risk, including the criteria that it uses, the roles and responsibilities of specific staff, the tools that will be used and the process that will be used.
Enterprise Risk Management Policy	Element of the Risk Management Framework documents – The ERM Policy details why Council manages risk. It affirms Council's commitment to risk management and reflects the value it places on the management of risk throughout the organisation.
Enterprise Risk Management Process	The systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk.
Enterprise Risk Management Procedure	Element of the Risk Management Framework documents – The ERM Procedure details how Council will undertake the risk management process.
Inherent Level of Risk	The true or real level of risk to the organisation. It is the level of risk prior to taking into consideration the treatment/controls that are currently in place to address the risk.
Key Performance Indicators	Are used to measure the performance of the organisations risk management activities and in the monitoring of risk exposures.
Level of Risk	Is the level of risk (ie. extreme, high medium or low) that is determined by utilising a risk matrix during a risk assessment process after taking into consideration the likelihood and consequence of a risk or opportunity event.
Likelihood	Chance or probability of a risk event occurring.
Operational Risk	Risks or opportunities that may impact on an organisations core operational activities. These are risks that the organisation may be exposed to or opportunities that may be available whilst undertaking the day to day operational services.

Term	Definition
Project Risk	Risks or opportunities that could endanger or enhance the planned budget, outcome quality, timeframe or goals of an approved project or one that is under consideration.
Residual Risk	The remaining level of risk after current risk treatment/control measures have been taken into consideration.
Risk	The effect of uncertainty on objectives. An effect is a deviation from the expected – positive and/or negative. Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances or knowledge) and the associated likelihood of the occurrence.
Risk Acceptance	An informed decision to accept the consequences and the likelihood of a particular risk.
Risk Analysis	A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.
Risk Appetite	The amount of risk an entity is willing to accept or retain in order to achieve its objectives. It is a statement or series of statements that describe the entity's attitude towards risk taking.
Risk Assessment	The overall process of risk analysis and risk evaluation.
Risk Attitude	The organisations approach to assess and eventually pursue, retain, take or turn away from risk.
Risk Category	Refers to the type of risk or opportunity that exists within Council's operations eg Liability, financial, reputational, WHS, economic etc.
Risk Control	That part of risk management which involves the implementation of policies, standards, procedures and physical changes to eliminate or minimise adverse risks or to ensure an opportunity is realised.
Risk Criteria/Context	Terms of reference against which the significance of a risk is identified and evaluated. Will include the defining of the internal and external parameters to be taken into account.
Risk Evaluation	The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.
Risk Identification	The process of determining what can happen, why and how.
Risk Matrix	A matrix that is used during a risk assessment process. The matrix is used to determine the level of risk (extreme, high medium or low) after taking into consideration the likelihood and consequence of the risk or opportunity event.
Risk Oversight	The supervision of the risk management framework and associated risk management processes.

Term	Definition
Risk Profile	A description of any set of identified risks. The set of risks can contain those that relate to the whole organisation, part of the organisation or as otherwise defined.
Risk Register	A register (electronic or manual) that records Council's enterprise risk profile data whether it be Strategic, Project or Operational risks .
Risk Tolerance	The levels of risk taking that are acceptable in order to achieve a specific objective or manage a category of risk.
Risk Treatment	Is a risk modification process. It involves selecting and implementing one or more treatment options. Once a treatment has been implemented, it becomes a control or it modifies existing controls.
Strategic Risk	Risks or opportunities that may impact on the Council's direction, external environment and to the achievement of its strategic plans. These risks or opportunities will inhibit or enhance Council's ability to achieve its corporate strategy and strategic objectives with the ultimate goal of creating and protecting community and stakeholder value.
Stakeholder	Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity of the organisation.
Worker	Person who carries out work for Wentworth Shire Council, whether paid or unpaid, or directly or indirectly engaged. Includes an employee, labour hire staff, volunteer, apprentice, work experience student, subcontractor and contractor.

Appendix D - WSC Risk Exception Report Template

Risk Exception Report Template								
What's this Report for	New Very High Risk ○	New High Risk older than 2 months ○	New High Risk older than 3 months ○	Risk increased by 2 levels or more ○	**Department of Reporter**			
Risk Owner					**Date Risk Rated at current level**			
Risk #.	**Risk Name / Description**	**What changed to alter the risk rating?** *Causes, consequences, controls etc.*		**Is there a plan to mitigate the risk?** *If yes, attach with report*	**WHEN** will the plan be implemented	**Who will monitor** the plan progress?	**Monitoring frequency**	

Appendix E - WSC Risk Identification Template

WSC Risk Identification Template			
	Most likely Risk Owner		
	Why will this person be the Risk Owner?		
	Date risk identified		

Risk (What is it that might happen to prevent Council from achieving its goals)	What might **cause** a risk event? *Example list:* • *poor training* • *unqualified staff* • *wet weather* • *power loss*	What might the **impact** of a risk event be? *Example list:* • *loss of revenue* • *community complaints* • *increased hazard* • *data breach*	**Control Measures** (What controls exist or can be implemented to manage the situation?)

Wentworth
SHIRE COUNCIL

Our values: Honesty and Integrity | Accountability and Transparency | Respect | Quality | Commitment