RISK MANAGEMENT MANUAL

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 Manual

Index

Introduction

Wentworth Shire Council has a strong commitment to risk management. Council recognises that whilst risk is inherent in all its activities, the management of that risk is an integral part of good management practice and fully supports risk management as a central element of good business practice that allows for risks to be identified, analysed, evaluated and treated. Council recognises that while some risks cannot be fully eliminated they can be identified, controlled and managed to an acceptable level. Therefore, Council will adopt a risk management approach consistent with the *AS/NZS ISO 31000:2018 Risk Management* in all of its processes to undertake proactive risk management.

Risk Management is the combination of culture, systems and processes undertaken by Council to coordinate the identification and management of risk. Risk management activities inform decision making, supports the achievement of objectives and the prevention of harm.

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

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

A key component of this Risk Management Framework is Leadership and Commitment. The Australian Risk Management Standard specifically states that *"Top management is accountable for managing risk while oversight bodies are accountable for overseeing risk management". The Standard goes on further to say that "Determining risk management accountability and oversight roles within an organisation are integral parts of the organisation's governance".*

There are a number of terms and concepts that are often used to describe activities relating to managing risk. Understanding these will help Council manage risk more effectively. The following are some of the key terms and concepts covered in this document:

- risk
- risk-based decision making
- risk management
- risk management framework
- risk maturity.

Purpose

This Risk Management Manual confirms Council's commitment to improving its capability to identify and manage risks as an integral part of business practices.

In implementing the Risk Management Manual, it is important to ensure:

1. Risk management practices support Council's Strategic Community Plan and other business plans;
2. A consistent and coordinated Council wide approach to risk management;

3. A risk aware workforce and an environment that supports informed and responsible risk behaviours to protect the community, employees and contractors;
4. Council risk areas are identified; significant risks are assessed and appropriate controls and treatments are put in place to minimise adverse impacts and ensure opportunities can be realised;
5. Governance and compliance requirements for risk management are met; and
6. Accountability through informed risk decision making and resourcing.

Key terms

Term	Definition
Consequence	Outcome of a risk event affecting objectives
Enterprise Risk Management (ERM)	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.
Level of Risk	The ERM Policy details why Wentworth Shire 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.
Likelihood	Chance or probability of a risk event occurring
Operational Risk	Risks or opportunities that may impact on an organisation's 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.
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'
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.

Term	Definition
Risk Register	A register (electronic or manual) that records Council's enterprise risk profile data whether it be Strategic, Operational or Project 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.

Risk

"Risk is the effect of uncertainty on objectives."

The effect that uncertainty has on the achievement of Council's objectives, gives rise to risk. It is measured in terms of consequence and likelihood. Council will be exposed to risk from many sources such as: political, economic, social, technological, regulatory or environmental. There are many different types of risk, positive, negative or both, and can address, create or result in opportunities and threats. There are also multiple factors that influence risk. These may be global or localised and within Council itself. Some factors will be beyond Council's ability to influence or control but Council may still be impacted.

The positive aspect of risk is the "risk/reward" concept, where the benefits of taking a risk outweigh the potential negative impacts. Council will accept risk in order to achieve or exceed its objectives, provided there is an understanding of those risks and they are guided by Council's risk appetite and managed in accordance with this framework.

To manage risk, it is important to understand how uncertainty and objectives influence risk:

Uncertainty

There is no absolute certainty about the future but there is generally a level of predictability to outcomes and performance. Uncertainty reduces the predictability, in turn giving rise to risk. As uncertainty changes, so does the risk. This means risk is dynamic and needs to be monitored and reviewed on a regular basis.

Common sources of uncertainty

When something is not available, unreliable or invalid; where the interaction or relationship is unknown, is variable or can be interpreted differently; when something is random, inconsistent; or has a range of possibilities and changes over time. Assumptions and presumptions are also a common source of uncertainty.

Objective

A clear understanding of the objective is important to risk identification. If there is a lack of clarity about what Council is trying to achieve, it can result in a risk being identified that is not an actual risk. This can have flow-on consequences, such as unnecessary investment in controls and resources and underlying exposures left unidentified and unmanaged.

An objective can be a personal objective, daily objective or an objective that relates to the outcomes Council wants to achieve. The objectives of Council are the expression of intent and purpose that generally relates to enabling legislation, strategy and visions.

In Council there a multiple strategic, operational and project objectives. Executive and senior managers have a role to manage conflict or dependencies between objectives and find ways to address any uncertainties.

When considering risk:

- define the objective to determine the risk(s);
- consider the objective in a future context;
- identify what is uncertain about the objective;
- formulate a view of why it is important to achieve the objective;
- identify and manage through the risk management process;
- consider resources required to manage risks; and
- assess future requirements as priorities change.

Risk-based decision making

Decisions are often made based on incomplete information and where the outcome is uncertain. For example, they may be based on the best available information at the time, and a reliance on assumptions, research, evidence or past experience.

Risk-based decisions however, are where risk management as a discipline is applied to the decision-making process. This means taking into account the uncertainties of the potential choices and considering the effects and impact of actions before making a decision.

Understanding how much risk Council is prepared to take is a useful way to help make a risk-based decision. If there is limited tolerance for a risk, it provides good guidance on what decisions cannot be made. Conversely, where Council is prepared to take some risk within its mandate and legislative obligations, it provides decision makers with more confidence.

There are essentially two types of risk-based decisions:

- Informal – where there are conversations and discussions involving routine day to day activities of Council.
- Formal – is generally applied to key activities and objectives with a defined process and approach.

Risk Management

"Coordinated activities to direct and control an organisation with regard to risk"

Risk management is used to describe the activities undertaken by Council to identify, assess and manage its risk. Risk management is fundamental to improving performance and achieving outcomes. When routinely applied, informed decisions can be made with more confidence.

Risk management is most effective when:

"every person thinks about risk and manages risk as part of their job."

Risk management cannot prevent every risk from occurring due to the uncertain nature of some risks.

Risk management will:

- Develop a discipline to avoid or reduce the likelihood and potential impact(s) of a risk;
- Provide a level of comfort that informed decisions are being made; and
- Ensure the Council is doing all it reasonably can to manage its risk.

Risk management supports an assessment and decision regarding:

- What risk to avoid;
- Why some risk can be taken; and
- How risk must be managed.

Risk management includes the approach, process and activities undertaken to ensure that:

- Adequate oversight, reporting, monitoring and assurance occurs;
- Risks are identified, assessed and action taken;
- Controls are identified, assessed and sufficient investment occurs; and
- People have the right capability and skills to manage risks.

Why Risk Management is Important

Risk management applied as a discipline within Council's prescribed risk management framework will:

- Support successful execution of strategy, business plans and projects;
- Increase the chance of achieving objectives;
- Improve culture;

- Provide confidence to the Council and the community;
- Promote the efficient allocation of resources;
- Reduce negative perceptions and impact on reputation;
- Empower people to make decisions with confidence;
- Determine how much risk can be taken and tolerated; and
- Inspire others to follow examples and work collaboratively.

Managing risk means managing the effect of uncertainty to provide greater assurance that Council will achieve its objectives by minimising threats and seizing opportunities. This requires directing, controlling and holding Council accountable for:

- Systematically identifying the risks in all aspects of Council's operations that can affect achieving objectives; and
- Making informed decisions about these risks.

Successful management of risks will, amongst other things:

- Reduce foreseeable threats to a level that Council is willing to accept; and
- Enable you to maximise opportunities that may present themselves.

The successful management of risk will increase the likelihood of Council achieving its objectives, both in the short and longer term. A robust risk management framework, by increasing Council's resilience and capacity to learn, will support the sustainability of Council.

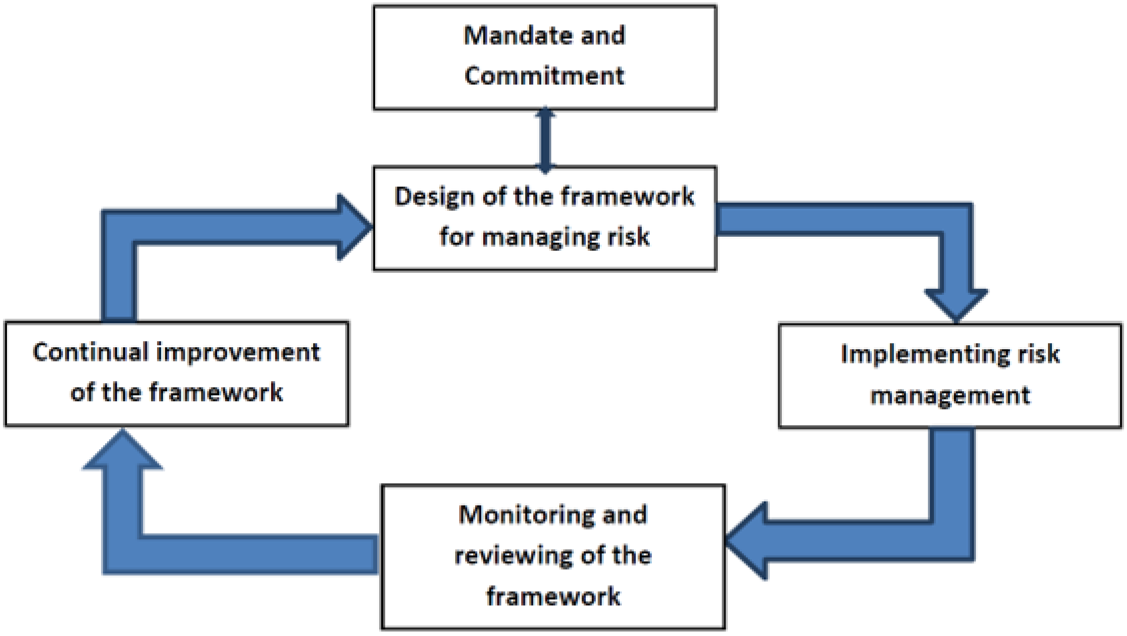
Risk Management Framework

A risk management framework is the set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

It is the totality of all processes, procedures, documents, policies, resources, governance and arrangements that Council has in place that contributes to managing risk. A framework is essential to ensure there is an agreed approach to manage risk. It is required as part of overall governance arrangements and will also complement and support other frameworks.

The risk management standard sets out the components of a risk management framework. While Council will have processes and approaches in common with other councils, all councils are different due to their mandate and requirements. This means that Council's approach to risk management should be developed and tailored to suit its specific requirements.

The core components of ensuring an effective risk management framework are per the diagram below:


Mandate and Commitment
Design of the framework for managing risk
Implementing risk management
Monitoring and reviewing of the framework
Continual improvement of the framework

Mandate and Commitment **What is it?** It reflects the intent to ensure effective risk management. **Why is it important?** It provides the basis for a common and consistent approach. **How is it evident?** When commitment to risk management is strong and supports a positive risk culture.	**Typically, this would be reflected in:** • mission and value statements • policies • position descriptions • continuous improvement plans	**Council will:** • endorse the risk management policy • ensure a positive attitude towards risk management • review regularly the effectiveness of its risk management framework.
Design **What is it?** It reflects what is required and what should be included. **Why is it important?** It considers context, requirements and components. **How is it evident?** Design of the framework enables a systematic and structured approach.	**Typically, this would be reflected in:** • risk management procedures • governance structure • risk management policy • terms of reference of committees • communication and consultation plans	**When designing the framework Council has taken into account:** • internal and external factors. • accountability and responsibility for managing risk • integration into corporate and business planning • communication and reporting mechanisms
Implementation **What is it?** It reflects what actions are required to make it real. **Why is it important?** It ensures planned activities occur and are resourced. **How is it evident?** Implementation and integration of the risk management framework supports risk-based decision making across Council.	**Typically, this would be reflected in:** • risk management plan • project documentation • risk management policy • corporate and business plans • minutes of committee meetings • budgeting and planning process • procedure manuals associated with management systems • risk management training systems • internal audit and assurance plans	**Council will:** • develop a risk management plan to support integration. • identify requirements for building internal capabilities • review its progress. • report outcomes • re-assess progress at least annually.

Monitor and Review **What is it?** It reflects the approach required to assess performance. **Why is it important?** It ensures effective and fit for purpose. **How is it evident?** Monitoring and reviewing the risk management framework continuously ensures it is effective and supports performance.	**Typically, this would be reflected in:** • a risk management plan • a risk management attestation statement • a risk management policy • terms of references of committees • minutes of committee meetings • risk management KPI's • risk assessments • internal and external audit reports	**Council will:** • assess its risk management framework at least annually. • monitor progress against the risk management plan. • implement enhancements as required.
Continual improvement **What is it?** It reflects the continual improvement process. **Why is it important?** It ensures it is dynamic and aligns to requirements. **How is it evident?** Implementing a risk management improvement plan continuously enhances risk management and risk.	**Typically, this would be reflected in:** • a risk management plan • a risk management attestation statement • a risk management policy • minutes of committee meetings • risk management KPI's • risk assessments • audit reports	**Council will:** • develop a risk management plan • incorporate improvement activities into its Continuous improvement plan • measure improvement through monitoring and assurance.

The benefits of a robust risk management framework are:

- Achieving and maintaining compliance with all laws, regulations, policies and procedures;
- Reliable, timely and accurate financial and management reporting;
- Efficient, effective operations and resource use, including safeguarding assets from misappropriation and misuse;
- Achieving and maintaining conformance with best practice and standards;
- Maintaining business continuity;
- Maintaining the community's confidence in the services that are delivered;
- Adapting to changes in the political environment;
- Minimising negative impacts of Council's activities on the environment;
- Maximising the benefits of relationships with other public and private sector organisations;
- Adapting to changes in communities and to community needs and expectations; and
- Ensuring the safety and wellbeing of the workforce;

DEVELOPING AN EFFECTIVE RISK MANAGEMENT FRAMEWORK

Risk governance

Council will:
- develop a risk management plan;
- ensure roles and responsibilities are well defined and included in position descriptions;
- commit to improving, monitoring and measuring risk culture;
- assess its risk appetite and incorporate it into decision making and corporate planning; and
- develop an approach that provides assurance to Council that risks are being managed.

Process

Council will:
- establish and communicate its process;
- develop appropriate tools and templates;
- ensure people have adequate skills and capability;
- develop escalation protocols;
- ensure risk appetite is defined in its risk criteria;
- invest in control assessment and management; and
- align internal auditing to monitoring risk.

Resources

Council will:
- invest adequate resources into the function;
- support independence and escalation of risks;
- assess capability requirements and link it to development plans;
- create opportunities for people to champion risk; and
- provide adequate training and learning opportunities

Risk Profile Review

This is a formal process where Council's risk profile is reviewed periodically and annually.

This involves a requirement to:
- collect evidence of the identification, evaluation and review of risks and their controls;
- assess effectiveness that is supported by audit activities and data to provide assurance;
- review and sign-off of the process by risk owners;
- escalate any deficiencies and failures in systems or processes with recommendations for future actions;
- assess that the process has been adopted and implemented; and
- check that there is evidence of:
    - governance, systems and reporting;
    - risk identification and understanding of Council's risk profile and management plan;
    - assurance activities;
    - failures and deficiencies identified and escalated for further actions; and
    - continuous improvement in managing risks which are dynamic and changes as the

Risk Maturity

Risk maturity describes the capability and level of maturity that Council operates at in terms of its risk framework. Risk maturity is linked to Council's performance and achievement of outcomes.

Risk maturity typically encompasses all elements of the risk management framework. There may be varying levels of risk maturity across different elements within the framework.

Risk maturity is not a static concept and is susceptible to internal and external factors and drivers over time. As Council's context changes, risk management also needs to evolve to ensure that it continues to support the achievement of objectives.

The desired level of risk maturity should be considered by the Council, which is aligned to achieving strategic objectives and managing its risk profile. The desired risk maturity should be reflected in Council's risk management plan to influence risk improvement activities.

Council will consider developing and implementing strategies to improve its risk maturity or maintain it at the desired level. Continual improvement is a fundamental element for effective risk management. Council will develop its approach to risk management over time and invest adequate time and resources to achieve its desired rating.

Risk maturity goes beyond the structural elements of ensuring a framework is in place. It also requires Council to determine if it is effective. This means Council will need to assess whether:

- risk management is contributing to its overall performance;
- the risk management function is operating as expected; and
- outcomes are being achieved.

Risk Maturity Assessment

An assessment of risk maturity enables Council to assess the performance of the risk management framework and to determine whether it is meeting expectations. An assessment provides a roadmap for improvement through identifying opportunities to mature the framework to the desired level. Council will undertake a self-assessment of its risk maturity using the model defined in the risk management standard.

Risk Management Principles

Risk management principles are not compliance-focused. They provide a set of statements to guide and assist in the design, implementation and oversight of Council's risk management framework. Reference to decision making, human behaviour and cultural factors includes ensuring risk management is operating as intended and contributes to improved performance and outcomes.

Risk Management	How is it Applied?	Why is it Important?
1. Creates and protects value	• Incorporated into governance framework • Considered as part of organisational culture	• Contributes to the achievement of objectives • Assists to improve performance • Protects community interests
2. Is an integral part of Council's planning and management process	• Integrated into strategic and business planning • Informs delegations • Part of change management process	• Avoids duplication • Guides prioritisation • Clarifies responsibilities
3. Is part of decision making	• Built into approval processes • Explicitly incorporated into projects, system design and changes and resource allocation • Part of all contract agreements • Part of staff recruitment and employment arrangements	• Assists decision makers to make informed choices • Assists to prioritise actions • Distinguishes among alternative courses of action
4. Explicitly addresses uncertainty	• Used to develop descriptions for risk rating criteria (likelihood and consequence) • Linked to assessing objectives	• Explicitly identifies uncertainty in Council's internal and external contexts • Promotes a shared view of risk and risk appetite • Identifies vulnerabilities
5. Is systematic, structured and timely	• Incorporated into the design of all systems rather than a stand-alone process • Consistently applied through clear guidance • Measured and reported	• Contributes to a consistent and efficient approach • Facilitates comparability of results and benchmarking • Promotes consistent understanding
6. Is based on best available information	• Advice and support for risk management is available • Specifies the functional requirements of risk management systems • Used to accurately define uncertainty and ensure treatments are relevant	• Stakeholders require accurate and reliable data to manage risk • Risk attestation is supported • Evaluates the effectiveness of controls • Develops risk monitoring and reporting • Risk management information systems are fit-for-purpose

Risk Management	How is it Applied?	Why is it Important?
7. Is tailored	• The risk framework is designed and operated to fit with Council's context and capabilities	• Aligns with Council's external and internal context and risk profile • Consistent with Council's culture • Adequate resources are allocated • Complies with legal obligations
8. Takes human and cultural factors into account	• The risk framework considers how people and cultures interact with its functions and how to monitor risk cultures and behaviour	• Aligns the capabilities and intentions of stakeholders with Council's objectives • Ensures consistency between culture and behaviour
9. Is transparent and inclusive	• Identifies scope and method for risk monitoring and reporting to stakeholders • Identifies elements required in the risk criteria • Identifies the role of stakeholders in the risk management process	• Promotes line-of-sight of risks between all levels of Council • Facilitates appropriate and timely involvement of stakeholders • Ensures that the risk management plan remains relevant and up to date
10. Is dynamic, iterative and responsive to change	• Incorporated into change management strategies • Incorporated into strategic and business plans	• Build's Council resilience • Ensures plan takes account of emerging risks • Ensures the risk management framework is responsive to changes in context
11. Facilitates continual improvement	• Risk management system is incorporated in continual improvement systems • Risk attestation and the results of internal audit are used to inform continual improvement • Stakeholder feedback is sought to influence the ongoing development of the risk framework	• Improves Council's risk maturity • Addresses stakeholder expectations to protect community interests • Assists Council to meet obligations.

Risk Governance

Risk governance refers to the culture and arrangements developed by Council to manage the uncertainties to achieving its objectives. It includes the leadership, accountabilities and oversight that builds and improves the risk management approach.

Risk governance is an essential part of Council's overall governance responsibilities. Effective risk governance supports Council to improve performance and achieve outcomes as it will:

- Guide required risk management behaviours;
- Establish consistent processes; and
- Drive informed decision making

Council has adopted the three lines of defence model. This model is most effective when there is active support and guidance from the Council and senior management.

Each of the three lines has a distinct role in Council's governance and oversight. The Council, the Audit, Risk & Improvement Committee and senior executive are considered the primary stakeholders that are served by the established lines. This means they are in a position to ensure that the three lines of defence are reflected, enacted and reviewed as part of Council's risk management control processes.

Collectively they have responsibility and accountability for setting Council's objectives, defining strategies to achieve those objectives, and establishing governance structures and processes to best manage the risk in accomplishing those objectives. The three lines of defence model is best implemented with the active support and guidance of the Council, the Audit, Risk & Improvement Committee and the senior executive.

The three lines of defence model distinguishes among three lines involved in effective risk management:

- Functions that own and manage risk;
- Functions that oversee risks; and
- Functions that provide independent assurance

The first line of defence: operational management

As the first line of defence, operational managers own and manage risks. They are also responsible for implementing corrective actions to address process and control deficiencies.

Operational management is responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis. Operational management identifies, assesses, controls and mitigates risks, guiding the development and implementation of internal policies and objectives.

Operational management naturally serves as the first line of defence because controls are designed into systems and processes under their guidance of operational management. There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight control breakdown, inadequate processes and unexpected events.

The second line of defence: risk management and compliance functions
Management establishes various risk management and compliance functions to help build and/or monitor the first line of defence controls. The typical functions in this second line of defence include:

- A risk management function that facilitates and monitors the implementation of effective risk management practices by operational management and assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout Council.
- A compliance function to monitor various specific risks such as noncompliance with applicable laws and regulations.
- A controllership function that monitors financial risks and financial reporting issues.

Each of these functions has some degree of independence from the first line of defence, but they are by nature management functions. As management functions, they may intervene directly in modifying and developing the internal control and risk systems. Therefore, the second line of defence serves a vital purpose but cannot offer truly independent analyses to the Council regarding risk management and internal controls.

The responsibilities of these functions vary in their specific nature, but can include:

- Supporting management policies, defining roles and responsibilities, and setting goals for implementation;
- Providing risk management frameworks;
- Identifying known and emerging issues;
- Identifying shifts in Council's implicit risk appetite;
- Assisting management in developing processes and controls to manage risks and issues;
- Providing guidance and training on risk management processes;
- Facilitating and monitoring implementation of effective risk management practices by operational management;
- Alerting operational management to emerging issues and changing regulatory and risk scenarios; and
- Monitoring the adequacy and effectiveness of internal control, accuracy and completeness of reporting, compliance with laws and regulations, and timely remediation of deficiencies.

The third line of defence: internal audit
Internal audit provides assurance on the effectiveness of governance, risk management, and internal controls, including the manner in which the first and second lines of defence achieve risk management and control objectives. The scope of this assurance, which is reported to senior management and to the Audit, Risk & Improvement Committee and the Council, usually covers:

- A broad range of objectives, including efficiency and effectiveness of operations; safeguarding of assets; reliability and integrity of reporting processes; and compliance with laws, regulations, policies, procedures, and controls;
- All elements of the risk management and internal control framework, which includes: internal control environment; all elements of Council's risk management framework; information and communication; and monitoring; and
- The overall entity, departments and functions – including business processes as well as supporting functions such as human resources, information technology etc.

Internal audit actively contributes to effective Council governance by fostering its independence and professionalism.

First Line: Management Control	Second Line: Risk Control and Oversight Functions Established by Management	Third Line: Independent Assurance
Controls are designed into systems and processes under managerial guidance. Adequate managerial and supervisory controls are required to ensure compliance and to identify breakdowns or unexpected events. Operational managers are responsible for: • Owning and managing risk and guiding development of internal policies and procedures and ensuring activities consistent with objectives; • Implementing corrective actions to address process and control deficiencies; • Maintaining effective internal controls; and • Executing risk and control procedures on a day-to-day basis. Team leaders design and implement detailed procedures that serve as controls and supervise execution of those procedures.	Risk management function (and/or committee) facilitates and monitors the implementation of effective risk management practices in the following way: • Supports management policy; • Monitors risk management and provides guidance and support; • Assists risk owners and management; • Identifies and alerts management to shifts and emerging issues; • Monitors specific risks, adequacy of internal controls, reporting and compliance; and • Assists in the development of processes and controls Designed to ensure the first line of defence is operating as intended.	Internal audit is established to provide the Council and senior management with assurance around: • Effectiveness of governance and risk management; • Internal controls; • How first and second line of defence is operating; and • Assessment of control objectives and plans. **External auditors, regulators and external bodies** Those entities outside the structure of Council but who play an important role in the overall governance and control structure.

Corporate and business planning

Corporate and business planning refers to the annual planning Council undertakes at all levels to determine its objectives and develop supporting plans. Risk management must be incorporated into corporate and business planning processes as a mandatory requirement.

Incorporating risk management provides value to decision makers as it will:

- Identify what could impact Council’s objectives;
- Provide an opportunity to develop strategies to minimise the impact; and
- Support decisions on how much risk can be taken to achieve objectives.

If risk management is not incorporated it essentially means decisions are made that have not considered what is uncertain and the possible resulting effects, implications and dependencies.

Risk management in corporate and business planning includes the identification and validation of key risks to strategic objective and risks associated with organisational or department plans.

Risk management needs to be undertaken for projects, policy development and as part of the delivery of services. This will ensure there is a comprehensive consistent and integrated approach across the organisation. Failure to do so could result in gaps and unexpected exposures.

Risk Management Policy

Council has developed a risk management policy that outlines the intent of the organisation with respect to risk management and describes the governance arrangements and expectations. It provides guidance and is fundamental to establishing a positive risk culture in Council by clarifying expectations regarding the attitude, awareness and accountabilities related to risk management.

The policy has been endorsed and approved by the Council and will be reviewed annually or when there is significant change.

Risk Management Plan

A risk management plan describes Council's future vision, direction and objectives for risk management. It incorporates key activities designed to achieve these objectives and the plan to build risk management capability and maturity. The plan ensures that the Council and management have a common and clear view of the purpose of risk management, the activities to be pursued to enhance the framework and the capability building requirements to achieve this.

An effective risk management plan ensures the risk management framework is suitable to the context of Council. It enables Council to:

- Prioritise monitoring activities;
- Assist in the direction of resources to support gaps in risk management capability; and
- Strengthen its approach to continual improvement.

Council will consider its risk management plan development in line with its corporate planning cycle. A structured approach which involves a clearly documented plan, endorsed by the Council will be adopted.

A robust risk management plan will:

- Provide a common view of context, risk management capability and maturity;
- Define the vision, objectives and future direction of risk management;
- Ensure risk management is aligned to the context and corporate objectives;
- Establish a plan to address risk management capability gaps;
- Assist with prioritising the risk management framework monitoring and assurance activities; and
- Align to the continual improvement approach.

Risk Culture

Risk culture refers to the behaviours that lead to how every person thinks and manages risk. Risk culture is a component of the overall culture of Council. The risk management framework supports the development of a positive risk culture within Council.

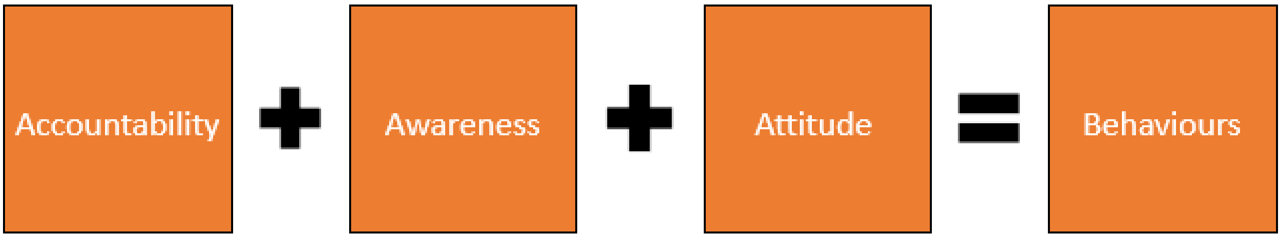
The Council and senior executive are responsible for setting the “tone at the top”. They play a key role in influencing and articulating the desired risk culture. Developing a positive risk culture is essential to developing risk maturity and building capability. It is important because it will:

- Create the tone and set expectations;
- Modify behaviour to what is expected within Council’s values and behaviours; and
- Underpin risk-based decision making.

Developing a positive risk culture requires a continuous improvement approach. This will ensure people are provided with opportunities to grow and improve their risk management capability and knowledge. It will also support consistent and appropriate risk decisions.

Risk culture encompasses how risk management is embodied and includes:

- **Accountability** – the way in which accountabilities are communicated and managed.
- **Awareness** – how aware people are of the risk management framework.
- **Attitudes** – the attitude towards risk management and its value proposition.



Accountability + Awareness + Attitude = Behaviours

The following provides guidance on the three components for developing a positive risk culture.

Accountability	Awareness	Attitudes
The Council and senior executive take leadership responsibility for risk management.	**Risk management is at the front-end of decision making and aligned to objectives.**	**Risk management is viewed as everyone’s responsibility.**
• Obligations, delegations and accountabilities are documented and communicated • Commitment and ‘tone from the top’ are widely understood and consistently applied • Intent is reflected in values and behaviours are consistently applied • Reporting is transparent and timely • Performance mechanisms support and reward positive risk behaviour • Roles, responsibilities and ownership are documented and communicated • Risk culture is evaluated and aligned to the risk management plan.	• Risk management policy and procedures are readily available • Integrated into corporate and business planning cycle • Applied as part of day-to-day decision making and activities • Standard approaches and access to supporting documents and tools • Common vocabulary is developed and understood • Obligations, delegations and accountabilities are understood and applied • Roles, responsibilities and ownership are understood and accepted.	• Risk management function has influence • Value is expressed through discussions, actions and activities • Ongoing learning supports improvement initiatives • Staff feel free to challenge and escalate • Staff operate with delegations • Council’s values are evident in staff’s behaviour • Ethics and integrity underpin activities

Risk Appetite

Risk appetite refers to the type and amount of risk that Council is prepared to accept or avoid in pursuit of its objectives. It encourages the consideration of risk in strategic and operational decisions by asking:

"Is this course of action compatible with our risk appetite?"

Council's risk appetite statement is the shared view of the Council as the governing body and senior executive on the nature and amount of risk it will retain or accept to achieve its strategic objectives.

The risk appetite statement influences and guides decision making, clarifies strategic intent and ensures choices align with the capacities and capabilities of Council. It supports a shared understanding of:

- Opportunities and uncertainties;
- What type of risk to pursue;
- How much risk to accept;
- What risk can be tolerated; and
- Investment required.

Mandate, legislative requirements and stakeholder expectations affect how much risk Council can accept. Expectations are set by the Council and agreed to with senior executive. The executive communicates expectations to ensure monitoring, reporting and reviewing occurs.

Defining risk appetite will:

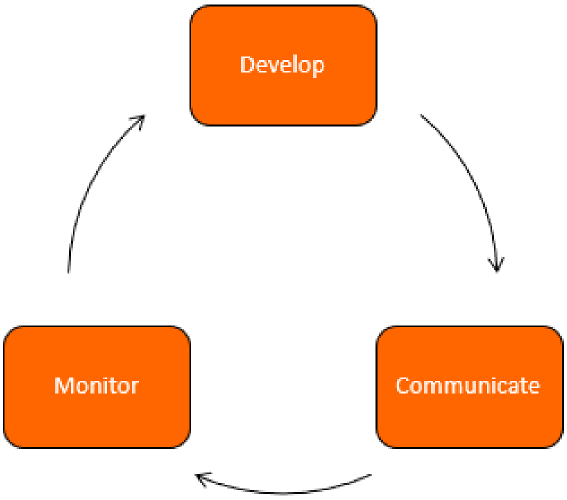
- Focus on what is important to Council;
- Develop a shared view of risk;
- Promote risk-based decision making; and
- Improve oversight and monitoring.

A risk appetite statement supports:

- Defining new initiatives and project priorities;
- Corporate and business planning and reporting; and
- Investment and resource allocation.

Steps in determining risk appetite

A statement can be a high-level statement or include expectations for particular risks.



Develop

- Design statement to suit Council
- Define against key strategic objectives
- Clear statements for decision makers

Communicate

- Set the tone for risk management
- Ensure risk criteria reflects risk appetite and tolerances

Monitor

- Include in risk reporting
- Review and adjust as the internal and external environment changes
- Incorporate into continuous improvement activities
- Utilise internal audit to review

Develop	Communicate	Monitor
Identify key stakeholders who need to contribute to the development of the risk appetite statement.	Identify key internal and external stakeholders who need to be aware and apply the risk appetite statement.	Confirm governance arrangements for oversight of the application and impact of the risk appetite statement.
Identify expectations of stakeholders and their general attitude of the risk profile and its capacity to bear the risk. Using surveys or event-based scenarios may assist with this.	Establish the preferred methods for communicating with each stakeholder group.	Ensure adequate systems (technology) to facilitate monitoring, timely reporting and escalation when tolerances are exceeded.
Identify and agree on points in the business where key decision making is pivotal, so that risk appetite can be applied at those points.	Establish the content and form of risk appetite communication.	Ensure corrective actions to address variations are identified and implemented and that progress is reported.
Identify how risk appetite performance will be monitored.	Review risk criteria to ensure it reflects risk appetite and tolerances.	
Identify the limits for each risk appetite statement.	Confirm that the performance of the risk appetite statement will be monitored by the Council.	
Identify the thresholds for each risk statement • Acceptable • Tolerable • Unacceptable		
Identify the specific events that will trigger a review of the risk appetite statement.		

Risk Reporting

Risk management reporting is the regular provision of risk information to enable decision makers to fulfil their risk management obligations.

Accurate and timely reporting of risk information, particularly to internal stakeholders, is essential to good corporate governance. Information on current and emerging risks, and treatment and monitoring plans should be used in strategic planning, departmental, operational and project management processes to provide reasonable assurance that Council's objectives are being met.

The Director Finance & Policy as the head of Council's Risk Management function has the overall responsibility for producing reports. The frequency and content of reports will be tailored to the needs of individual stakeholders.

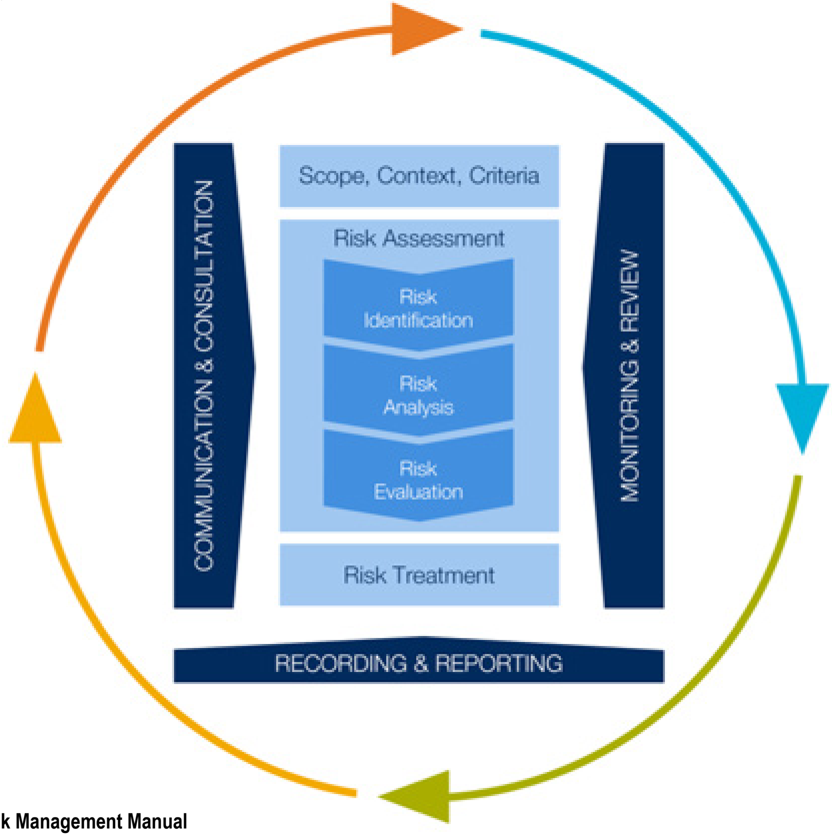
While the risk standard focuses on residual risk, in reporting and documenting risks it may sometimes be good practice to also consider 'inherent risks' (risks assuming no related controls), in addition to 'current risks' (risks after current controls) and residual risks. This will provide stakeholders, including the Audit, Risk & Improvement Committee, with a complete picture of all risks and a position on which to challenge management on the effectiveness of controls.

Risk Management Process

The risk management process is a core component of the risk management framework. Having a documented risk management process is important as it will outline the steps about how to:

- Establish the context
- Understand what is uncertain and potential effects
- Identify and assess what could happen
- Make a decision about what needs to occur

Key Steps of the Risk Management Process



Communication and Consultation

Staff should communicate and consult with stakeholders at all stages of the risk management process. Effective communication and consultation mechanisms will support the effective implementation of Council's risk management process.

Staff may wish to perform a stakeholder analysis to develop a deeper understanding of the issues that most concern stakeholders, their level of influence and the impact that Council has on them. Staff can conduct a stakeholder analysis for the whole department, a specific department or business function, or as a part of the development and implementation of a particular project.

Consultation

There is a need to consult with internal and external stakeholders so that:

- The context in which Council is operating is fully understood;
- The interests of stakeholders are understood and considered;
- All risks are identified;
- Different areas of expertise are drawn on when analysing and evaluating risks;
- Different views are considered; and
- Staff can secure endorsement and support for risk treatment plans.

Consultation can be formal or informal. Formal consultation processes may include strategic planning sessions, presentations to the executive; internal memoranda, minutes from relevant risk evaluation meetings, surveys and focus groups. Formal consultation ensures stakeholders needs and concerns are addressed in a structured environment, and establishes an audit trail of decisions.

Informal consultation may include less formal meetings, workshops, emails, updates, reports, briefings and interviews

Communication

Clear and effective communication is necessary to ensure that those responsible for implementing risk management receive the right information at the right time, so they can make the best decisions and carry out their risk management responsibilities.

Different stakeholders within Council will have different information needs. For example, staff who are accountable for carrying out actions to deal with risk will need to understand their accountabilities, the rational for decisions and why these actions are required.

Other internal stakeholders such as the General Manager, the Council and advisory committee such as the Audit, Risk & Improvement Committee and senior management will have their own unique information needs, such as an understanding of how risks are managed and reported.

Staff also need to communicate information about risks and how they are being managed to external stakeholders. For example, through progress reports to funding bodies.

Communication with your stakeholders should be continuous, and should permeate the risk management process.

Staff will need to develop plans to identify what, how, when and to whom you will communicate information about risks and the risk management process. These communication plans should be developed early in the risk management process. The plans should be regularly reviewed and revised to ensure they reflect changes in the external, internal and risk management contexts.

Establish the Context

Establishing the context is about defining the external and internal parameters to be considered when managing and setting the scope of the risk management process.

This step is essential to determine:

- The objective(s) being achieved;
- Why and what type of risk assessment is required;
- What information is required to understand the risk – both internal and external; and
- What subject matter experts should be consulted.

In practice, there are essentially two ways the risk management process occurs in Council:

Informal Risk Management Process	Formal Risk Management Process
A formal documented risk assessment process has not occurred but the risk is considered and some action may be taken. Informal risk management process may occur during day-to-day activities where there is some uncertainty that may affect what Council is trying to achieve.	A coordinated approach where the steps of the risk management process are followed and applied. This can occur in a structured discussion, workshop or meeting and can often be facilitated. It will result in risk(s) being recorded and actioned with an owner, time frames, reporting and monitoring.
The following may occur: • Discussions of potential future risks of concern are discussed either with a manager or colleague and this leads to a change to a work practice or process. • Discussions of a potential future risk of concern occur and specialist expertise is sought. • Discussions occur where there has been a change in the context or environment and there may be a heightened monitoring of the situation. • A trend in incidents is identified and there may be a need to assess the potential for a risk to an objective emerging. • Discussions of an emerging issue or risk is escalated and considered for formal assessment. • A standard meeting agenda item could include identification of potential risks or emerging issues for discussion and/or action, which could include escalation.	A formal risk assessment may occur for: • Defined objectives important to the successful execution of Council's strategy and operations. • Projects. • New services. • Government initiatives or policy directives. • Change in Council's mandate or requirements. • Identified problems that require further assessment and/or analysis. • Inter-Council matters, agreements or requirements.

Establishing the external context

The external context is the external environment in which Council operates. Defining this context requires consideration of the impacts that external factors may have on operations and the ability for Council to achieve its objectives. This can include the following:

- Political – change of government, change in government policies
- Economic – economic growth, commodity prices, interest rates
- Socio-cultural – population growth, impact of demographic change on demand for services, change in stakeholder expectations, community groups
- Technological – technological change, cost of updating technology, obsolescence of systems
- Laws and regulations – legislation, regulations and standards
- Environmental – impacts that Council operations have on the built or natural environment, climate change.

It is important to identify the key trends and drivers as well as considering stakeholder perceptions and values and how these may influence the ability to achieve Council's objectives.

Establishing the internal context

The internal context is the internal environment in which Council's operates. Defining the internal context requires consideration, amongst other things of Council's objectives, structure, capabilities, processes and stakeholders. Areas to consider include:

- Organisational structure
- Organisational culture
- Risk culture – including risk appetite and risk tolerance
- Internal stakeholders (e.g. staff, volunteers)
- Capabilities of Council (e.g. staffing, Councillors, work areas, sites, IT systems etc.)

Establishing the context of the risk management process

The risk management context refers to the parameters established for each individual risk management process based on a consideration of Council's external and internal environment. Establishing the risk management context within Council requires the need to consider, and determine:

- Council's goals, objectives, strategies, resources and accountabilities for its risk management activities;
- The risk management methodologies to be used;
- The risk criteria to be used to measure risk and determine if a given risk is acceptable or tolerable; and
- The performance metrics to be used to evaluate the risk management performance.

The use of consistent terminology and language is important with following terms commonly used in risk management:

- **Consequence** – the outcome of an event affecting objectives
- **Control** – a measure (including a process, policy, device, practice or other action) that modifies risk
- **Event** – an occurrence or change of a particular set of circumstances
- **Level of risk** – the magnitude of a risk, or combination of risks, expressed as a combination of consequences and their likelihoods
- **Likelihood** – the chance of something happening
- **Risk** – the effect of uncertainty on objectives
- **Risk tolerance** – Council's readiness to bear the risk that remains after risk treatment in order to achieve its objectives.

Developing risk criteria
One of the reasons for establishing the context is to allow for the development of risk criteria for Council. There is a need for a set of standard criteria so that everyone in Council has a common understanding of how to evaluate the significance of a risk. Risk criteria consists of scales to measure consequence, likelihood, control effectiveness and the overall level of risk, and to determine Council's response to different levels of risk.

Although risk criteria are initially developed as part of establishing the context for risk management, they should also be further developed and refined as particular risks are identified, and risk analysis techniques are chosen or as Council's risk management maturity grows.

Measuring consequences
There are many techniques for measuring consequences. Techniques range from qualitative methods, which use a set of descriptors of the level of risk (e.g. very high, high, medium, low), to quantitative techniques, which are based on statistical analysis of historical data.

Designing consequence tables
A consequence table enables Council to measure consequences using a consistent, predetermined scale. It consists of a matrix that defines consequence levels for each consequence type.

The three main steps in creating a consequence table are:

1. **Identify types of consequences that should be included in Council's table;**
2. **Determine how many levels of consequences Council need in the table to differentiate severity; and**
3. **Describe each consequence level for each consequence type.**

The steps for creating a consequence table are discussed in detail below.

Step 1: Identify types of consequences that should be included in the table
The first step is to identify all types of consequences that will affect Council's ability to achieve its objectives. Consequences tables need to include the most relevant types of consequence that may be experienced by Council, based on its understanding from establishing the context.

Both tangible (such as financial) and intangible (such as reputational) types of consequences should be considered.

Council has chosen the following consequences:

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

Step 2: Determine how many levels of consequences are needed in the table

The next step is to determine the number of levels required to describe severity for each of the consequence types identified in the previous step. The aim is to define enough levels to clearly differentiate the levels of severity for each consequence. Be careful not to specify too many levels as this may make it difficult to choose the most appropriate consequence level, particularly between adjacent levels. Similarly, if there are too few levels, it may also be difficult to choose the most appropriate.

Council has chosen five consequence levels:

- Extreme
- High
- Medium
- Minor
- Insignificant

Likelihood table

A likelihood table can be used to define the levels of likelihood of a given event that Council will use to analyse risks. Likelihood can be defined quantitatively or qualitatively.

The three main steps in defining likelihood are:

- **Determine how many levels are needed in the table**

As with consequences, the aim is to define sufficient levels so that each risk can be assigned an appropriate likelihood rating. If too few levels are specified, it will make it hard to differentiate between likelihoods. If too many levels are specified, it will make it difficult to select the most appropriate likelihood rating, particularly when a risk straddles two likelihood levels.

- **Decide how to describe the likelihood**

Likelihood tables usually use terms such as rare, possible, likely and almost certain to describe the chance of something happening. A likelihood table describes each of these terms based on:

  - Frequency – the number of times that something might happen in a given timeframe, and/or
  - Probability – the chance of something happening on a scale from 0 percent (the event will not occur) to 100 per cent (the event will certainly occur).

As with consequence tables, the method used will be influenced by Council's risk management maturity, the type and reliability of data available, and the capabilities and experience of those who will be interpreting and analysing the data.

To define the likelihood of a risk, consideration needs to be given to all sources of the risk that could cause the risk to emerge.

- **Describe the levels of likelihood in a table**

Each level on the likelihood scale should be described so it is easily understood and unambiguous, using the method chosen in the previous step. Each likelihood should be clearly distinguished from the level above or below it.

If the decision is to describe likelihood levels in terms of both frequency and probability, there is a need to ensure that the descriptions for each level, whether in terms of frequency or in terms of probability, are broadly comparable.

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

Measuring the effectiveness of your controls

Council will need to establish criteria to measure the effectiveness of existing risk controls. Once the existing risk controls have been identified then they need to be assessed as follows:

- Whether the controls are well designed – are they capable of managing the risk and maintaining it at an acceptable or tolerable level?
- Whether the controls are operating as intended - have they been, or can they be, proven to work in practice? Are they cost-effective?

The assessment of existing controls can be qualitative, semi-quantitative or quantitative, depending upon data available. In many instances, a simple set of descriptors can be used to qualitatively assess control design and operating effectiveness.

Council's control effectiveness table is as follows:

Control Effectiveness Table			
Level	**Description and Further Action**	**Design Effectiveness**	**Operational Effectiveness**
Effective	Existing controls address risk, are in operation and are applied consistently. Management is confident that the controls are effective and reliable. Ongoing monitoring is required.	Y	Y

Control Effectiveness Table			
Partially Effective	Controls are only partially effective, require ongoing monitoring and may need to be redesigned, improved or supplemented.	N	Y
		Y	N
Not Effective	Management cannot be confident that any degree of risk modification is being achieved. Controls need to be redesigned.	N	N

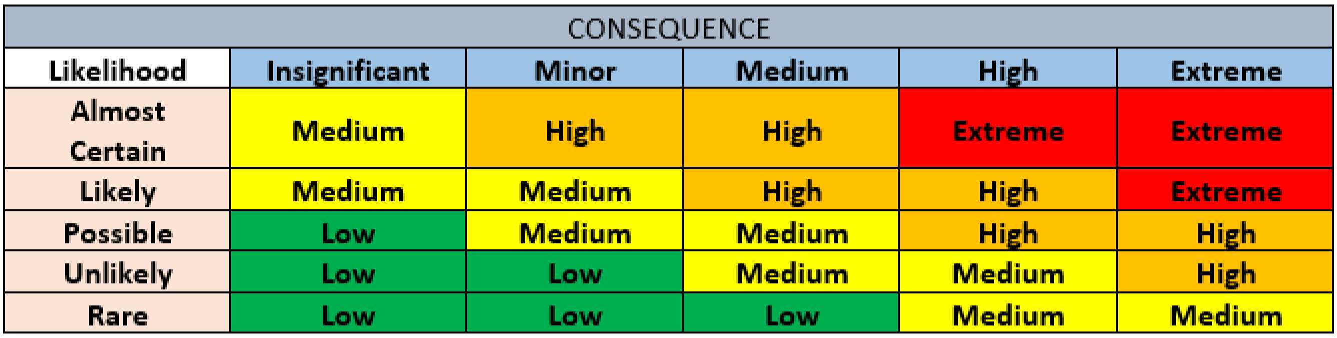
Where a control (or a suite of controls) have been assessed as ineffective, analysis should be undertaken to decide whether it would be better to improve the existing control(s) or replace them with a new control(s).

There may be more than one control for a particular risk. It may also be more useful to assess the effectiveness of all controls taken as a whole for a particular risk rather than to individually assess the effectiveness of each control separately and try to combine the results.

Council's Internal Audit function can also provide an objective assurance of the adequacy and effectiveness of controls.

Determining a Risk Level

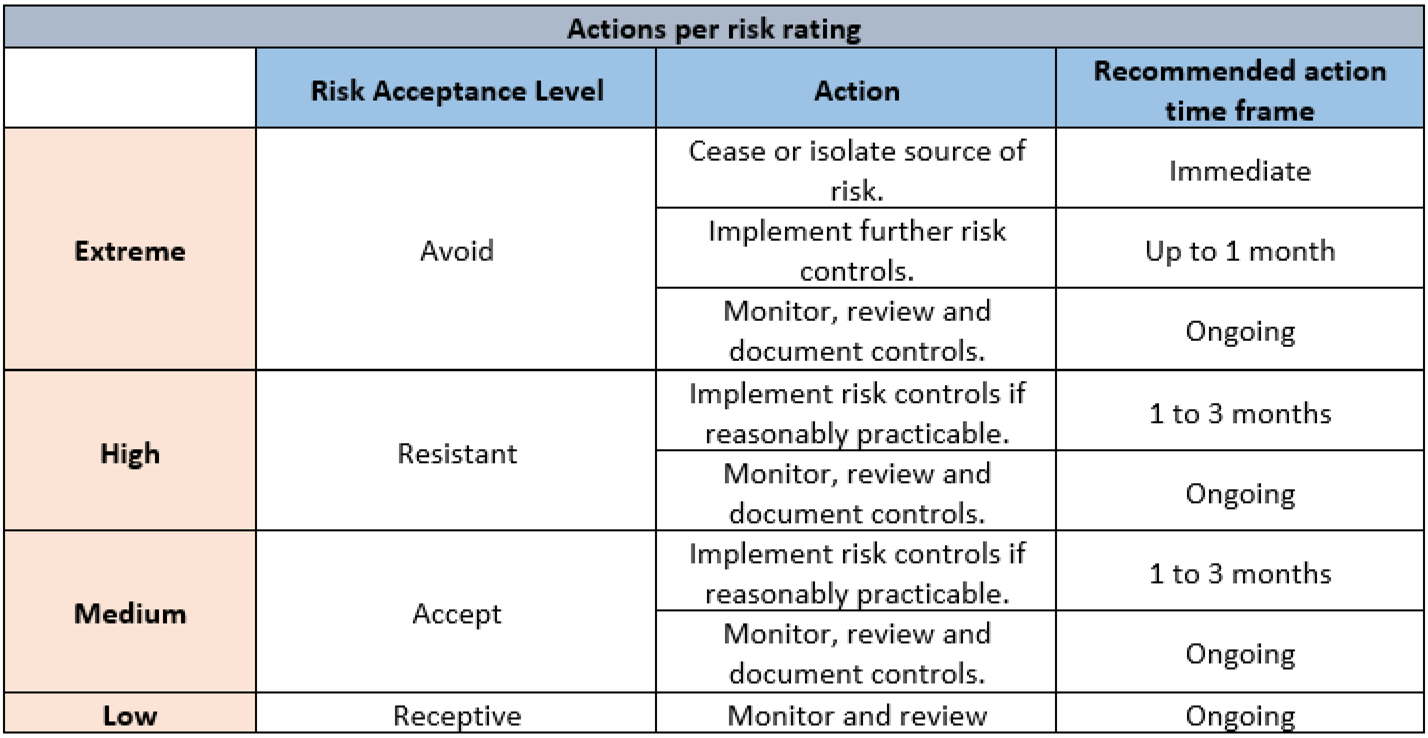
A common qualitative technique is the use of a risk matrix. A risk matrix provides a graphic representation of the relationship between consequence, likelihood and the resulting risk level. Each square in the matrix represents a unique pairing of consequence and likelihood and, therefore a risk level. 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

Multiple risk levels have been grouped and colour coded into extreme, high, medium and low categories. Each grouping is associated with a decision rule, such as treat the risk to bring it to an acceptable level, treat the risk only under certain circumstances or accept the risk.

These groups can also provide escalation points for risk management decisions, ensuring that risks are visible to, and managed at, the appropriate level. Council has developed the risk action table:



Actions per risk rating

	Risk Acceptance Level	Action	Recommended action time frame
Extreme	Avoid	Cease or isolate source of risk.	Immediate
		Implement further risk controls.	Up to 1 month
		Monitor, review and document controls.	Ongoing
High	Resistant	Implement risk controls if reasonably practicable.	1 to 3 months
		Monitor, review and document controls.	Ongoing
Medium	Accept	Implement risk controls if reasonably practicable.	1 to 3 months
		Monitor, review and document controls.	Ongoing
Low	Receptive	Monitor and review	Ongoing

Developing a hierarchy of risks in Council

Each function and department need to identify risks through their planning process and their day-to-day operations. In certain circumstances there may be a need to develop consequence and likelihood and risk matrices that are more appropriate to the particular circumstances.

The reason being that what may be a high risk at a particular function or department level, maybe a lower risk at an overall Council level. This is particularly important at a project level; therefore, it is important for project-specific consequence tables and set escalation levels to ensure that major project risks are escalated to the appropriate level.

Determining Council's tolerance for risk

All organisations are exposed to a range of risks (both opportunities and threats) of varying severity arising from a number of internal and external sources. While Council can avoid or mitigate some threats, it is usually necessary to tolerate a level of risk in order to achieve a level of benefit.

When determining at what level Council is prepared to accept or tolerate a specific risk without developing further strategies to modify the level of risk, the following should be considered:

- The specific nature of the risk;
- The operating environment of the risk;
- Any legislative or organisational obligations;
- The type of consequence from the risk; and
- Internal and external stakeholders, their perceptions of risk and how much risk they are prepared to allow Council to accept.

It is important to ensure that there is a common awareness of the level of risk that Council is prepared to accept or tolerate. This will enable consistent decision making when managing risk.

By clearly defining the risks that Council will accept or tolerate, enables Council to improve its ability to deliver on services by:

- Providing input for the decision-making processes;
- Showing how different resource allocation strategies can add to or reduce the total burden of risk;
- Identify specific areas where risk should be removed; and
- Increasing the transparency and consistency of business decisions.

The overall risk that Council faces is a combination of all the individual risks that it has to deal with as it strives to meet its objectives. Council's overall risk should not exceed the total burden of risk that the organisation is prepared to accept or tolerate. It is therefore important to take a holistic view of the organisation's risks.

Understanding the level of risk Council is prepared to accept or tolerate is generally an evolving process, where changes occur over time and with changing staff, systems, community expectations, cultures and technology. Executive and senior management levels must conduct regular discussions to ensure that risk management strategies remain appropriate. All staff should be aware of the actions required at different levels of risk. Council has developed the following risk tolerance statements as outlined in the Enterprise Risk Management Policy:

In exercising its functions under the *Local Government Act 1993*, Council has an appetite for accepting risk that appropriately balances the rights, expectations and quality of life of the people it serves, with the obligation:

a. to provide a safe working environment for its staff; and
b. to provide continuity and sustainability in the provision of services and growth of the organisation.

As such appetite for taking risk can vary across these different areas, therefore Council's risk appetite statements have been developed against each of Council's risk categories. These statements are qualitative in nature and designed to provide an indication of Council's general position when deciding to take or retain risk, in pursuit of its objectives.

These statements use a four-level ordinal scale to indicate the amount of risk Council is willing to take or retain for each category. The four levels are as follows:

- **Avoid** – (little to no appetite) – Avoidance of adverse exposure to risks even when outcome benefits are higher;
- **Resistant** – (small appetite) – A general preference for safer options with only small amounts of adverse exposure;
- **Accept** – (medium appetite) – Options selected based on outcome delivery with a reasonable degree of protection; and
- **Receptive** – (larger appetite) – Engagement with risk based more on outcome benefits than potential exposure.

Each category has been given a primary and a secondary appetite. These positions are defined as follows:

- **Primary Appetite** – Indicates a general appetite for taking or retaining risk for the given risk category.
- **Secondary Appetite** – Indicates an appetite by exception position for taking or retaining risk in specific circumstances

Council expects the General Manager to provide it with ongoing assurance that the organisation has suitable processes in place to appropriately identify and manage all strategic, operational and project risks, within the following tolerance levels:

Risk Category	Risk Appetite Statement
Reputational	Council is responsible for making decisions that adequately service the community as a whole, but is aware that all decision carry a degree of risk that segments of the community will disagree with. Consequently, in the current operating environment Council is willing to **Accept** risk where there is a reasonable degree of protection for achieving the desired outcome. However, in some circumstances Council's appetite will become more **Resistant** to risk exposure and Council will actively attempt to limit adverse risk exposures.
Financial	As a general position Council is **Resistant** to taking risks in its financial activities to achieve its objectives and prefers to take safer options in order to ensure long term financial sustainability. Council will, however **Accept** some risk to ensure outcome delivery where reasonable protections are in place.
Natural & Environmental	In consideration of its commitment to the natural environment of the Wentworth Shire, Council tends to be **Resistant** to taking risk in pursuit of its environmental objectives and prefers to limit its risk exposures whilst maintaining the environmental resilience of the region. With the exception of very specific circumstances, Councils appetite for taking risk does not change, and Council remains **Resistant** to large risk exposures and prefers safer options.

Risk Category	Risk Appetite Statement
Security & Operational	As a general position, Council is willing to **Accept** appropriate levels of risk with regard to the delivery of services in the Wentworth Shire as long as the focus remains on outcome delivery and reasonable protections can be maintained. However, in specific circumstances, for short periods, Council will adopt a more conservative position and endeavour to **Avoid** decisions that would adversely increase its exposure.
Legal, Regulatory & Political	Council is **Resistant** to taking on, or retaining risk relating to its Legal, Regulatory and Political processes. Council will seek, practicable options that limit exposure in this area. In some circumstances Council will be more conservative and prefer to **Avoid** risk exposure even if the potential for favourable outcome benefits is considered to be high.
People	As a general position Council will **Avoid** taking risks that compromise the wellbeing and safety of its staff, stakeholders and the wider Wentworth Shire community in order to achieve outcome delivery and will seek practicable options that limit exposure in this area. With the exception of very specific circumstances, Council's appetite for taking risk does not change, and Council will endeavour to **Avoid** large risk exposures and prefer safer options.

Risk Assessment

A Risk assessment is a structured approach to identify and analyse the uncertainties that exists in meeting Council's objectives. Risk assessment consists of three discrete stages:

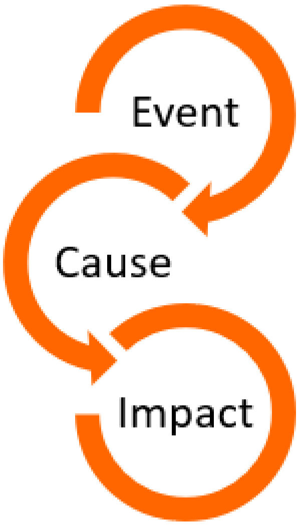
- Risk identification
- Risk analysis
- Risk evaluation

Risk Identification

Risk identification defines the "risk" problem and provides insight into "uncertainty" and the possible effect on the achievement of objectives. A well-described risk is important to provide context and meaning of the cause, event and impact for management and oversight. Key reasons are that it will:

- Assist to direct controls assessments and treatment planning;
- Provide meaningful information for reporting and oversight;
- Reduce over and under investment in unnecessary controls; and
- Align the uncertainty to an objective(s).

Risk will have a source and the following are the three key elements of a risk:



Describing a risk can be challenging and may take multiple attempts and a lot of discussion to agree on the risk. Breaking the risk up into three elements helps to:

- Identify the cause of the event to help determine what controls would be required;
- Understand the "something" that could happen to consider the possible impact; and
- Explore the potential impacts of the event to inform what decision is required.

Common pitfalls

There are some common pitfalls in relation to describing a risk, these include:

- Identifying risks as broad statements
  - Broad statements are less informative and difficult to manage at both an operational and strategic level.
- Identify risks as a cause
  - A cause contributes to a risk event occurring, rather than the risk itself. Articulating risks in this matter hinders the effectiveness of monitoring and measurement activities.
- Identify risks as incidents
  - Incidents are risks that have materialised. Treatment plans would be focused on managing the incident rather than preventing the incident from occurring again.
- Identify risk as consequences
  - Consequences may be measureable but cannot be managed effectively as they do not represent a specific "risk" event
- Identify a risk as a "type" of risk
  - Such as Occupational Health and Safety or Information Technology.

Risk analysis and evaluation

These are separate steps in the process but are usually undertaken together. Risk analysis is the process of coming to an understanding about the nature and level of risks so that a decision can be made about whether a risk needs to be treated and analysed to:

- Identify source and cause;
- Assess current controls, effectiveness and determine gaps;
- Consider how likely are/what are the impact(s); and
- Determine the risk rating = likelihood x consequence

Since the risk management process has inherent uncertainties, it is important that these uncertainties and sensitivities are identified and documented. The effectiveness of risk management is dependent on sound risk assessments. The process of undertaking risk assessments is ultimately an activity that requires subjective judgement. Although there may be other causes for faulty risk assessments, cognitive biases can be particularly pervasive.

If unchecked, these biases can lead to systematic decision-making errors and faulty risk assessments. Cognitive biases include:

- **Anchoring:** relying too heavily, or 'anchoring', on one aspect or piece of information when making decisions;
- **Bandwagon (or herd) effect**: doing (or believing) something because many other people do (or believe) the same;
- **Confirmation bias:** looking for evidence to justify preconceived ideas;
- **Framing effect bias:** arriving at conclusions based on how information is presented; and
- **Optimism (over-confidence):** overestimating the likelihood of favourable outcomes.

Recognising these biases is the first step in minimising their impact on risk assessments.

Evaluate to:

- Escalate to necessary reporting levels;
- Prioritise risks;
- Consider options;
- Describe what action is required; and
- Identify resources required

Risk evaluation is the process of deciding which risks require further treatment and in what order. It is based on the outcomes of the risk analysis. It involves determining where a particular risk, after existing controls are applied, sits compared with the level of risk Council is prepared to accept or tolerate, and the need for and priority of further treatment.

This evaluation of risks could lead to a decision to:

- Treat the risk without further analysis, or
- Consider the risk as insignificant and not warrant treatment, or
- Continue to undertake a more detailed analysis of the risk

Controls

A control is a:

"measure that is modifying risk – controls include any process, policy, device, practice or other actions which modify risk. Controls may not always exert the intended or assumed modifying effect."

Controls influence how a risk is rated. A risk may be rated too high or too low based on how the control is viewed, its effectiveness or in the absence of a control. Understanding the control environment is an essential part of the risk management process. The risk owner is the best person to provide a view of the control. Specialist expertise may be required to support and validate this view.

Controls are important because Council cannot operate effectively without appropriate governance structure, processes and procedures. Council will have controls to govern and guide the way it operates and delivers its services. Controls are generally the responsibility of risk owners and would include their oversight and implementation.
Some common controls include:

- Legislation;
- Delegations;
- Committees;
- Reporting;
- Policies, procedures, guidance material;
- Qualifications;
- Credentialing;
- Insurance;
- Employment screening;
- Training and professional development;
- Position descriptions;
- Values and behaviours, code of conduct;
- Audit, reviews, investigations;
- Equipment, devices, infrastructure; and
- Checklists, templates.

When analysing and evaluating a risk, consideration is given to the specific controls that are currently in place that would modify the risk. Considering both the design and operating effectiveness of controls is a critical aspect of the risk management process.

Multiple controls may exist and some will be more important or effective than others. Failure of controls could lead to an event. Key fundamental questions to consider are:

- What are the current control(s) in place that would modify this risk?
- Why is this control important in modifying this risk?
- How effective is the control at modifying this risk?
- Who is going to assess whether the control is effective?

Where there are multiple controls, it is important to identify the important ones or the ones that are critical. This is important to help make a decision about what action is required or about additional investment.

Council has adopted the following control effectiveness rating approach to guide the process and how controls should be rated. This will be supported by an internal audit program that is aligned to the risk register and risk plan.

Effective	Partially Effective	Not Effective
• This control is 100% effective	• This control is 50-75% effective	• This control is not effective at all

After the controls have been identified, assessed and rated, a decision can be made as to whether additional controls are required. Common issues with controls are:

- Defects;
- They deteriorate over time;
- There is uncertainty with the assumption when the controls were designed; and
- Changes in the environment in which they operate.

Management assumptions about the strength of internal control can influence the risk profile. Assumption should be tested to improve the design and/or effectiveness of internal control. Mechanisms exist to assess controls and the methods used may differ. This can include:

- Self – assessments;
- Review of errors and incidents;
- Root-cause analysis;
- Insurance claims;
- Modelling; and
- Specialist review by trained auditors and assessors.

Risk Treatment

Risk treatment is the process of identifying, selecting and implementing responses to risk that fall outside the risk levels Council is prepared to accept or tolerate. These risks will have been identified as part of the risk evaluation process.

This part of the risk management process seeks to control these risks by developing a treatment that addresses underlying causes, assesses the treatment's effectiveness and, if the residual risk is still considered unacceptable or intolerable, generate an alternative treatment.

The evaluation of the effectiveness of existing controls, which should have been carried out as part of the risk assessment process, can assist in determining whether existing controls should be modified or new treatments introduced.

A number of generic options (which are not necessarily mutually exclusive) can be considered for treating risks, including:

- **Avoiding the risk:** Where the level of risk is unacceptable or intolerable and the means of control are either not viable or not worthwhile, it might be possible to avoid the risk, for instance, by not proceeding with an activity that could generate the risk;
- **Changing the likelihood:** Developing and implementing strategies to change the likelihood of the risk occurring, either to reduce the change of negative outcomes or increase the chance of positive outcomes;

- **Changing the consequence:** Developing and implementing strategies to reduce the size of negative outcomes or increase the magnitude of positive outcomes;
- **Taking the opportunity:** Developing and implementing strategies to recognise, and benefit from, circumstances that offer opportunities, as well as strategies to exploit possible benefits while mitigating threats;
- **Sharing the risk:** The responsibility for treating risk can be either shared or transferred to other parties. This can be a good option to reduce Council's exposure to financial risk or asset risk. It is important to note, however, that transferring may not result in the complete transfer of a risk; and
- **Accepting or tolerating the risk based on informed decision:** This may be appropriate where the remaining risk levels are insufficient to justify potential treatment options or where it is not possible or is not cost effective to treat the residual risk.

The risk treatment itself could introduce secondary risks. For example, sharing or transferring risks raises a new risk in the organisation or department within Council with which the risk has been shared or transferred to may not manage the risk effectively. Secondary risks like this should not be treated as new and separate risks, but should be considered along with the original risk when developing a risk treatment.

Selection of risk treatment options
It may not be possible to eliminate all risk relating to Council's operations. Risk treatments need to be cost effective, practicable and commensurate with the level of the risk.

In selecting the most appropriate treatment or combination of treatments, Council needs to balance the costs and resource requirements against the likely benefits. Both financial and non-financial costs and benefits should be considered in making this assessment.

Since a chosen treatment might affect multiple risks there is a need to review the suite of proposed treatments to resolve any conflicts and eliminate any duplication.

Develop and implement risk treatment plans
Once selected, chosen risk treatments should be developed by risk owners into detailed risk treatment plans so that:

- Risk treatments can be implemented effectively and in a timely manner;
- Performance and success measures can be assigned for the risk treatment so that Council can monitor and review its ongoing effectiveness; and
- Council is able to demonstrate the application of risk management in the organisation.

Information documented in risk treatment plans should include:

- The rationale for selection of treatment, and the expected outcome of the treatment; it is important that decision makers are kept informed of the residual risk;
- Accountabilities and responsibilities;
- The actions to be undertaken to practically implement the selected treatment;
- Budgets and other resources required;
- Performance measures;
- Timeframe and critical implementation milestones; and
- Reporting, review and monitoring protocols.

Monitor and Review

Monitor and review is an essential ongoing component of the risk management process as it will:

- Detect any changes to the internal and external context;
- Identify emerging risks;
- Measure performance of risk treatments;
- Provide oversight and governance of risks and treatments; and
- Assess if the risk has changed and requires escalation, or is no longer valid and can be archived from the risk register

Practical tips

- Develop an approach to identify and assess issues that may influence a risk;
- Ensure additional controls are operating as intended before re-assessing;
- Consider additional treatments if current ones are not effective;
- Seek feedback on the quality of risk reporting and adjust as required;
- Undertake cost benefit analysis of controls to ensure optimal investment is occurring;
- Identify risks that can be archived during the review process; and
- Ensure appropriate linkage to continuous improvement and auditing systems for sustained monitoring and improvement.

Reviewing the risk management process

Council should continually review its entire risk management process to ensure that risk management strategies are appropriate and up to date. This can be done by considering issues at each stage of the risk management process such as:

Process Element	Issues for Review
Establishing the context	• Have there been changes in the external or internal context, and does Council's risk management context need to change to remain relevant? • Have the stakeholders who should be considered changed? • Have Council's stakeholders' preferences changed with regard to how Council manages risk?
Risk identification	• Are the sources of information used to identify risks still relevant and reliable? • Are changes required to the risk identification process? What effect will these changes have on the identification of future risks? • Are there any new or emerging risks that should be considered?
Risk analysis	• Are the assumptions about risk, and the assumptions upon which the risk assessment is based, still valid? • How fit for purpose are the tools Council uses in the risk analysis process? Are they still relevant? Are they being correctly applied?

	• Are those responsible for analysing risk and assessing controls doing so in a consistent manner? • Has there been any change in the likelihood or consequence of risks? • Is there any need to modify Council's risk assessment process based on actual experience?
Risk evaluation	• Are those responsible for evaluating risks doing so in a consistent manner? • Have Council's risks changed in priority reflecting any changes to Council's context?
Risk treatment	• How effective are Council's risk treatment plans? o Are the controls effective and fit for purpose? o Does the risk require further treatment or is there a need to change Council's control strategy? • Are staff following procedures? Is the control strategy supported by appropriate communication including documentation and training? Do the benefits of the risk treatment continue to justify the costs of the treatment?

Recording and Reporting

The risk management process and its outcomes should be recorded and reported through appropriate mechanisms and governance structures of Council. This will ensure effective transparency of the risk management function, aid in decision-making of Council's leadership and facilitate interaction with stakeholders.

Communication and Consultation

Communication and consultation occurs throughout the process in various forms as it will:

- Support stakeholder engagement and accountability in the process;
- Include the right people to help to reduce uncertainty;
- Provide information and reports to relevant stakeholders;
- Create opportunities to collaborate, advise and provide expertise to assist the process;
- Increase awareness of risk management and its value; and
- Improve the decision-making process.

Practical tips

- Develop approach and document it;
- Decide what should be communicated and to whom;
- Create a stakeholder communication plan if relevant;
- Identify expertise required to provide advice about a risk;
- Nominate experts or owners to provide context on the risk; and
- Advise outcomes and seek feedback

Risk profile

Risk profiles are summaries used to present an overview of information contained in risk registers. The aim of risk profiles is to promote consistent organisational understanding of significant risks and their controls. Risk profiles can:

- Summarise and add value to the information in risk registers for risk owners, executive management, Audit, Risk & Improvement committee, governing body and other relevant external stakeholders;
- Help identify the objectives associated with the greatest uncertainty (i.e. most at risk);
- Highlight significant risks and key controls;
- Track progress on the implementation and effectiveness of controls;
- Track how the organisation's risks change over time; and
- Inform continuous improvement in organisational performance.

Risk profiles can be developed for any level in Council, such as at corporate or department level, as long as you can map the risks at that level against a set of relevant objectives.

Strategic Risks

Strategic risks are generally those that relate to the corporate risks of Council. They tend to be longer term and/or are of strategic importance and can impact the strategic intent of Council. It is possible for some operational risks to be of strategic importance and be classified as strategic.

Strategic risk assessment

A guide to undertaking a strategic risk assessment:

- Ensure top down agreement for the approach;
- Incorporate it as part of the annual planning cycle;
- Develop necessary processes and procedures;
- Develop and communicate expectations to participants;
- Estimate time frames and develop a simple action plan to guide the process;
- Assign actions and follow up arrangements post session;
- Ensure risk owners are available to talk to their risk;
- Communicate outcomes and agreement;
- Consult effectively, particularly with key identified stakeholders; and
- Report and monitor outcomes.

The same approach can be adopted at the business unit and/or departmental level. The key difference is that stakeholders and risk categories may change. Business unit/departmental risks need to align to the strategic objectives.

Risk Register

A risk register is used to record risks and provide information to manage them. Risk registers provides a mechanism for documenting, managing, monitoring, reviewing, updating and reporting risk information. The following are the key elements that should be included in a risk register:

- Risk number and description including the cause of the risk;
- Category;
- Controls;
- Effectiveness of controls;
- Likelihood rating;

- Impact (consequence) rating;
- Inherent risk rating;
- Residual risk rating;
- Responsible person/owner; and
- Status of treatment plan.

Practical tips

- Describe risks so that they are meaningful;
- Review risks regularly and archive risks that no longer require active treatment;
- Consider how many risks can reasonably be managed by each risk owner;
- Determine which risks are really important; and
- Manage access to maintain the integrity of the content

Resources

Managing risk is everyone's responsibility. Effective risk management requires resources. It is now a mandatory requirement to allocate adequate resources to risk management. This means considering what is required to satisfy Council's obligations and accountabilities.

Council will need to constantly make decisions regarding what constitutes adequate resource investment and will need to consider how it can effectively meet its obligations and deliver its services.

The risk management function is most effective when it has independent oversight of the risk profile and risk management framework. The risk management function should:

- Assist the Council, the Audit, Risk & Improvement Committee and senior management to develop and maintain the risk management framework;
- Tailored to be the right size for Council;
- Ensure there are reporting lines to conduct its risk management activities;
- Define roles, responsibilities and authorities;
- Ensure staff possess the appropriate experience and skill;
- Provide access to required areas of Council;
- Require notification and escalation of matters of concern or that deviate from the agreed approach; and
- Create a level of independence to support the three lines of defence and overall governance.

Practical tips

- Adequate resources are committed in budgets for:
    - Risk management framework;
    - Improvement plan activities;
    - Corporate and business planning;
    - Risk management function;
    - Risk culture development;
    - Staff and tools;
    - Controls and assurance
- Capability requirements are assessed and programs are established to support development;
- Role of the risk management function is well defined, has influence and supports improvement; and
- Tools, templates, guidance and support is available and easily accessible.

Insurance

This section outlines why insurance is an important option to help protect Council from the financial risk of something going wrong.

Council must have appropriate insurances in place that reflect its risk profile. Insurance does not prevent something from occurring. If something unexpected does happen insurance means Council won't have to fund the full cost of the loss. The community benefits from Council being able to recover financially and it minimises the impact on consolidated revenue.

Not all risk can be covered by insurance as there are many risks that don't have a direct financial impact and alternative risk management strategies would be required. Risk based decisions can also be made to insure a risk, where a cost benefit assessment determines insurance is not the best option.

Key factors to consider include:

- Type, scale and nature of the risk;
- What risk Council is prepared to accept;
- Availability of alternative risk management and mitigation strategies;
- Level of insurance required based on Council's objectives, risk profile and tolerance;
- Past claims experience; and
- Availability and cost of cover.

Insurance may be a viable cost-effective option to reduce the financial impact for Council if the risk occurs. Insurance should not be the only option.

- Preventative or mitigating strategies should be considered to reduce the likelihood and/or impact.
- Provide a cost benefit analysis of potential actions.

Barriers to effective risk management

Risk management is unlikely to be effective if:

- **You do not strongly link it to Council's objectives**: if the risk management effort is focused solely on achieving regulatory or legislative compliance, there will be significant gaps. Risk management should focus on, and support the achievement of Council's objectives.
- **You do not have the right culture**: in addition to a strong commitment, and sustained and visible support from senior management, there should be broad engagement with risk management across Council. Risk management should be seen as the responsibility of all managers and staff. Council's culture should support and encourage individuals to actively identify and report risks.
- **You do not commit the required resources**: sufficient time, training and other resources must be devoted to risk management. In addition, Council's risk management process should be supported by a system to properly and effectively manage risk information.
- **You make risk management processes too complex:** if risk documentation and processes are unnecessarily complex, managers, staff and other stakeholders will be less likely to support implementation. Risk documentation and processes should consider and reflect the needs of Council's stakeholders.

- **Your risk treatments are not commensurate with the risk**: treatments need to be cost effective, practicable and commensurate with the level of risk.
- **You do not identify the right risks**: risk management should support good decision making. If the risks listed in the risk register are described incorrectly or are to broad or too low level, they will not support good decision making. It will be difficult for decision makers to make the correct decisions if they are overwhelmed by detail. Council's key decision makers need a concise list of risks that accurately reflects the most significant risks Council faces.
- **You do not acknowledge the likelihood of cognitive bias in decision making**: Decision-making errors and faulty risk assessments will result from risk identification and assessment that reflect subjective judgements that have not been challenged or tested. Sometimes these errors can persist for years. Recognising bias is the first step in minimising its impact on risk assessments.
- **You do not set clear responsibilities**: Risks and their management need to be clearly assigned to risk owners.

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**

Wentworth
SHIRE COUNCIL

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