Risk Management Framework

Name of policy:	Risk Management Framework		
Adoption by Council:	25 September 2025	Minute number:	22/255
Last review date:	July 2025		
Review timeframe:	4 Years		
Next scheduled review date:	June 2029		
Related legislation:	*Local Government Act 1993* *Local Government (General) Regulation 2021*		
Associated policies/documents:	AS ISO 31000:2018 Risk Management – Guidelines OLG Guidelines for Risk Management and Internal Audit for Local Government in NSW Hilltops Council Enterprise Risk Management Policy		
Responsible Directorate:	Corporate and Community		

Key Definitions

The key risk management terminology used within the Framework is defined at Annexure A.

Document Control

Version No.	Date	Revision Details	Author	Approver
1.0	June 2025	Hilltops Council Draft Created	Procurement & Risk Coordinator	
1.1	July 2025	Incorporated feedback from ARIC	Procurement & Risk Coordinator	
1.2	27 August 2025	Draft Risk Management Policy and Draft Risk Management Framework presented to Council for 28 day exhibition and submissions	Procurement & Risk Coordinator	Council
1.3	27 August 2025	Draft Risk Management Policy and Draft Risk Management Framework placed on 28 day public exhibition and submissions	Procurement & Risk Coordinator	Council 25/255
2.0	25 September 2025	No submissions received Draft Risk Management Framework adopted	Procurement & Risk Coordinator	Adopted 25/255

Contents

1. Introduction

Hilltops Council recognises that risk is inherent in carrying out all of its business strategies and operations and that without a robust system for identifying and managing risks, the organisation is vulnerable to uncertainties and lost opportunities and is unlikely to be resilient in the face of change or adversity.

Council will therefore seek to ensure that risk management is a key consideration in all business practices and decision-making processes. Council acknowledges that risk management does not only involve managing the adverse effects of risk, but it also means realising potential and beneficial opportunities for both Council and the wider community.

Council's Risk Management Framework will therefore provide the foundations and organisational arrangements necessary to embed a proactive, structured and consistent approach to risk management throughout the organisation.

Ultimately Council seeks to achieve an environment where, with the provision of ongoing guidance and training, Council staff retain the risk management skills to effectively contribute to the pursuit of objectives, whilst endeavouring to protect Council, its staff, its community, key stakeholders and natural and constructed assets from the adverse effects of risks.

Council will therefore communicate risk management and foster a vibrant risk management culture that empowers all staff to make well informed evidence-based decisions, prioritise actions and distinguish between alternative courses of action in their daily business activities so as to ensure positive outcomes for both Council and the community.

Council's Risk Management Framework will align with the requirements of the *OLG Guidelines for Risk Management and Internal Audit for Local Government in NSW* and the principles and processes defined in *AS ISO 31000:2018 Risk Management - Guidelines.*

Council will maintain a risk management framework appropriate to the size, culture and complexity of its operations and environment and through regular review Council will ensure that its Risk Management Framework continues to remain effective and relevant to the organisation.

Council will apply a staged approach to the implementation of this Framework in accordance with available resources and priorities.

2. Mandate and Commitment

Council's Risk Management Policy confirms Council's commitment at a strategic level to a proactive and structured enterprise-wide approach to risk management in accordance with the OLG Guidelines for Risk Management and Internal Audit for Local Government in NSW and *AS ISO 31000:2018 Risk Management - Guidelines.*

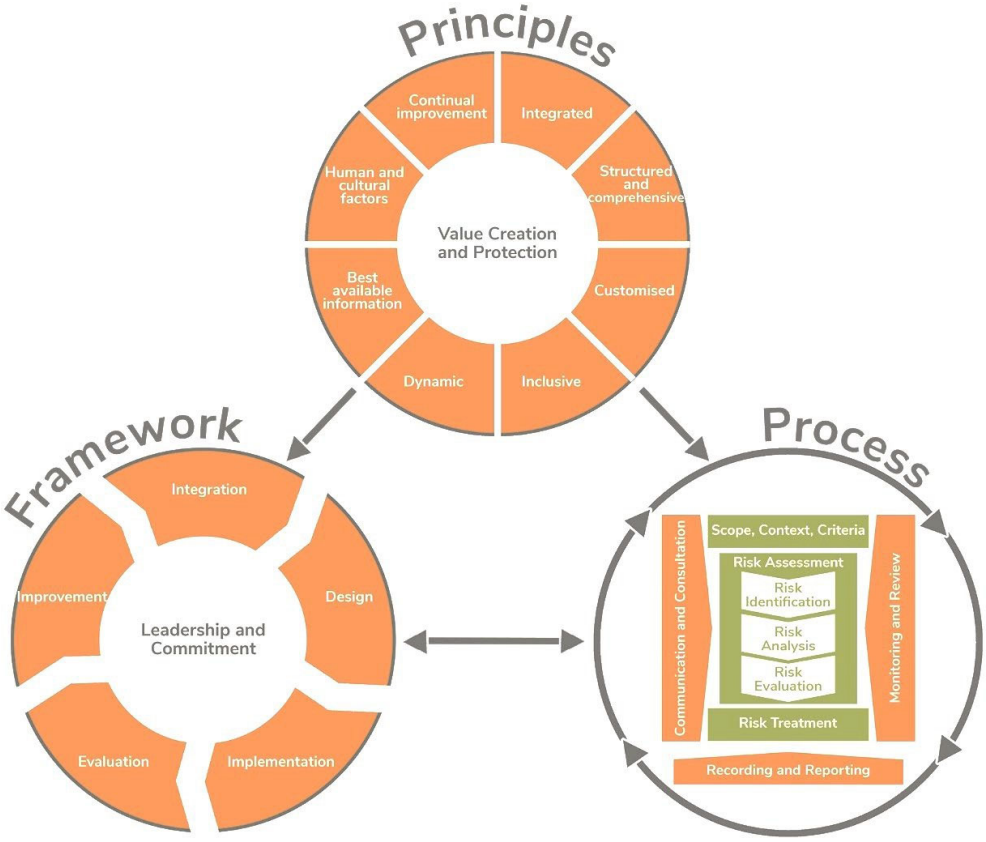
This Framework establishes Council's commitment to implementing appropriate risk management practices throughout the organisation in accordance with the Standard to achieve its risk management objectives.

3. Scope

Council's Risk Management Framework applies to all levels of the organisation - Council staff, management, Councillors, key stakeholders, contractors, service providers and the like. It extends to all of Council's current and future strategic and operational activities, business practices, policies, strategies, plans and procedures, as well as new opportunities for the organisation and the community.

4. Principles, Framework & Process

Council recognises the need to apply the Principles, Framework and Process detailed in *AS/NZS ISO 31000:20018 Risk Management - Guidelines* to ensure the management of risk in an efficient, effective and consistent manner.



5. Objectives

Through the implementation of an integrated and consistent approach to risk management, Council aims to achieve the following risk management objectives:

- An organisational culture of reliable, informed, evidence-based planning and decision making
- A consistent approach to the identification, assessment and treatment of risks
- Improved communication on matters of risk to enhance decision making
- Proactive and adaptive management practices
- Support achievement of Council's strategic objectives
- Effective allocation and use of resources for risk treatment
- Enhanced identification of opportunities and threats
- Enhanced organisational resilience and continuity of service
- Improved operational effectiveness and efficiency
- Staff accountability for risk identification and treatment
- Improved corporate governance, controls and performance
- Improved community and stakeholder confidence and trust by providing assurance that risks are appropriately managed
- Reduced liability exposure and financial loss
- Safeguarding of Council's resources - its people, finance, property and reputation

6. Implementation

In order to achieve its risk management objectives, this Framework will be implemented by undertaking the following activities:

- Integration of the risk management process into all Council strategic and business planning processes and associated plans and activities
- Defining a structured and consistent approach to the risk management process in accordance with *AS ISO 31000:2018 Risk Management - Guidelines*
- Providing easily accessible procedures, tools (risk assessment criteria) and guidance for staff to adequately identify, document, understand and manage risks
- Undertaking risk management education and training of staff at all levels of the organisation
- Establishing risk management resource to facilitate implementation of the Framework
- Defining risk management roles and responsibilities to ensure all staff manage risks relevant to their area of operation and accept accountability for their decisions
- Building a positive and proactive risk aware culture throughout the organisation
- Monitoring, reporting and reviewing risks on an ongoing basis
- Reviewing the Risk Management Framework in accordance with defined success measures
- Ensure that Council's Risk Management Framework informs its internal audit function.

7. Integration

Council will integrate risk management into its strategic and operational functions. Organisational strategies, plans and programs will be aligned with this Framework, including but not limited to, the in the following business areas:

- Strategic Planning
- Work Health and Safety
- Audit
- Asset Management
- Project Management
- Procurement
- Environmental Management
- Compliance
- Business Continuity and Disaster Recovery

8. Risk Management Culture

Council will effectively communicate and engage with staff at all levels of the organisation to build a positive risk aware culture that encourages all staff to proactively manage risks. Council will do this by:

- Ensuring Council's leadership promote and commit to risk management in a positive and proactive manner and communicate this with all staff
- Tailoring risk management training to ensure it is relevant to different levels of the organisation
- Engaging with staff about the benefits of risk management
- Communicating risk management roles and responsibilities
- Providing risk management support, ongoing guidance and resources to staff, including easily accessible risk management tools and systems
- Integrating risk management into strategic and business planning processes
- Participation in Statewide Risk Management Audits and regional risk initiatives.

9. Education and Training

Council will facilitate risk management training for staff in a manner that is commensurate with roles and responsibilities. Risk management training will be conducted as time and budget permits; however, guidance will be provided on an ongoing basis by Council's Governance & Risk Team. Council's training and guidance will include providing staff with the following:

- A general understanding of the principles and benefits of risk management;
- Practical guidance in undertaking and documenting the risk assessment process, using Council's adopted risk assessment and evaluation criteria, tools, templates and systems; and
- An understanding of Council’s risk appetite and actions required to effectively consider risk management options

10. Risk Categories

Council will undertake risk management with due consideration of the following adopted key risk categories:

Risk Category	Risk Description
Financial	• Financial decisions and performance of Council, including investment decisions and any finance decision that could/would potentially impact the financial sustainability of Council. • Council's financial health, stability, and sustainability. This includes revenue generation, budget management, investments, financial reporting, unforeseen expenditures, and potential financial loss impacting the Council's capacity to fund its services and obligations.
Governance and Legal	• The non-adherence to regulations, standards, codes of practice, or policies, leading to legal penalties, financial losses, or reputational damage. • Corporate Governance, including the efficient and effective direction and operation of the Council; ethical, responsible, and transparent decision making; corruption; fraud; procedural legal and legislative compliance.
Assets and Infrastructure	• Council's management and maintenance of its built environment, including (but not limited to) buildings, roads, bridges, pipe networks, footpaths, bike paths, parks, and sports/play infrastructure. • Public risk in the use of these assets
Environment	• Council's impact on the environment, as well as environmental factors affecting Council operations. • Compliance with environmental regulations, pollution, resource depletion, and the effects of natural climatic events and climate change.
People and Safety	• Internal Risks arising from Council workplaces, facilities, and operations that may affect employees, contractors, and volunteers. These include physical safety, psychological wellbeing, workplace behaviour, and compliance with Work Health & Safety legislation. • Third-Party Risks to members of the public, service users, and visitors resulting from Council activities, services, infrastructure, or events. These include potential injury, illness, or harm to wellbeing, as well as risks to vulnerable groups within the community.
Reputation	• Damage to, or fluctuations in, the reputation of Council with the community, other councils, and other levels of Government.
Growth	• Damage to, or fluctuations in, the reputation of Council with the community, other councils, and other levels of Government.

11. Risk Appetite

Council will have a responsible approach to risk management, seeking to recognise and manage its exposure to risks in accordance with its vision, mission and values. In pursuing the achievement of its objectives and governance responsibilities, Council will accept a degree of risk commensurate with the potential reward and with consideration of Council's role and responsibilities within the community. Council's risk appetite in relation to its adopted key risk categories is therefore as follows:

	Appetite or Willingness to Accept Risk			
	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.	**Receptive** (Larger Appetite) Engagements with risks based more on outcome benefits than potential exposure.
Financial	✓			
Governance and Legal	✓			
Assets and Infrastructure		✓		
People and Safety	✓			
Environment	✓			
Reputation	✓			
Growth			✓	

Council has no tolerance for risks that may compromise the safety and welfare of staff, the community, contractors and volunteers. Similarly, Council has no appetite for risks that cause significant and irreparable damage to the environment and seeks to preserve and enhance it for future generations

The tables below contain the “Primary” and “Secondary” Risk Appetite Statements for each Risk Category of Hilltops Council. These statements are qualitative in nature and designed to provide an indication of Council’s general position when deciding to take, retain or accept risk, in pursuit of its Strategic Objectives.

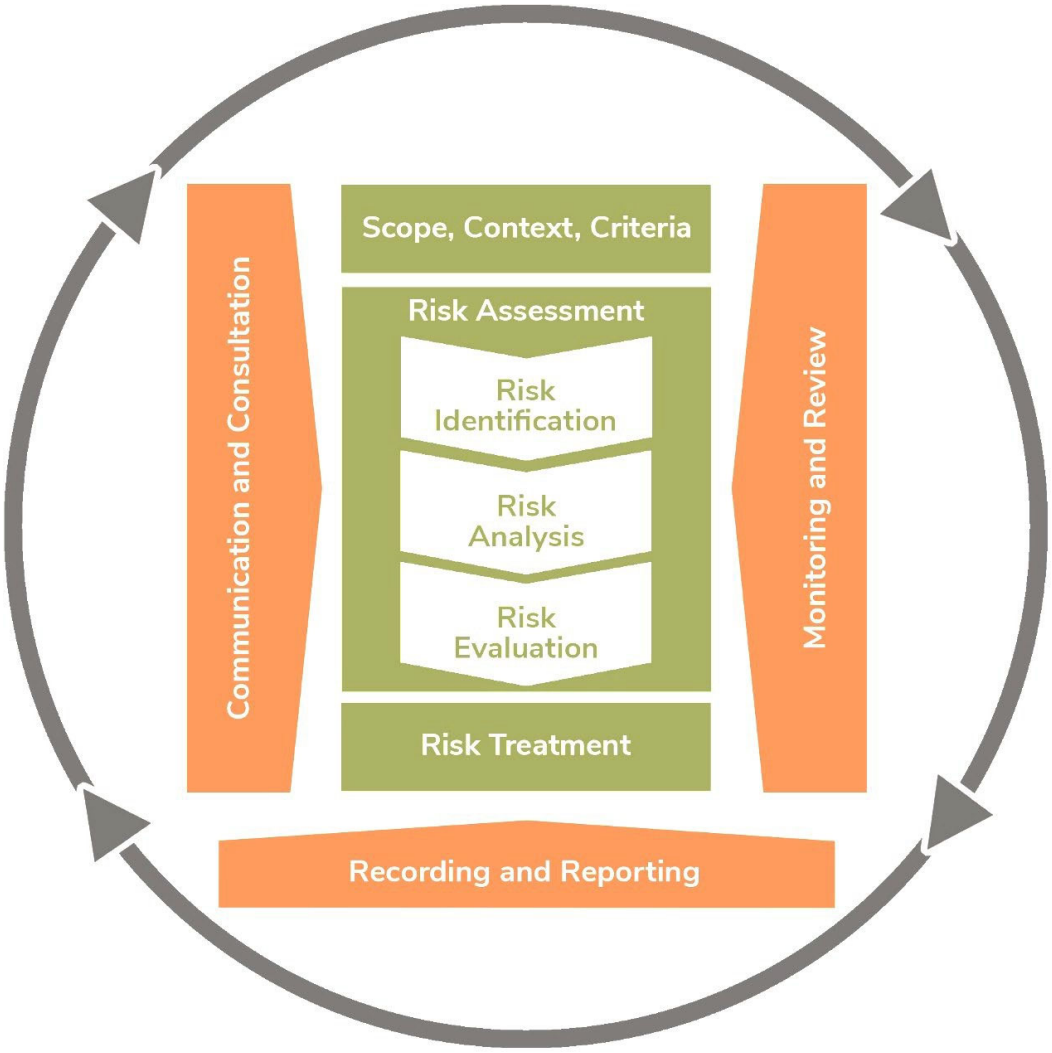
- Indicates the Secondary Risk Appetite

Category	Level	Risk Appetite Statement
Financial		
 Financial	Avoid	In an effort to achieve all of its Strategies, Council seeks to Avoid adverse exposures with its Financial activities. In some circumstances Council recognises that it may need to remain Resistant to risk but also take on a small appetite for risk with a preference towards safer options.
Governance and Legal		
 Governance / Legal	Avoid	In the pursuit of its Strategies, Council will endeavour to Avoid taking or retaining Governance/Legal risks. Council has little to no appetite for risk and prefers to avoid adverse exposures wherever practicable. Council does not consider that a secondary risk appetite level is necessary for this Risk Category.
Assets and Infrastructure		
 Assets Infrastructure	Resistant	Regarding its Assets/Infrastructure and achieving its Strategies, Council prefers safer options and is Resistant to taking, retaining or accepting risk. Council maintains a desire to limit itself to only small amounts of adverse exposure. Council does not consider that a secondary risk appetite level is necessary for this Risk Category
Environment		
 Environment	Avoid	In an effort to achieve its Strategies, Council seeks to Avoid as much risk as is practicable and limit adverse exposures when dealing with the Environment and environmental stewardship. In certain circumstances, Council will be less conservative but remain Resistant to Environment risks where the potential benefits warrant an increase in exposure and safer options can be maintained.
People		
 People and Safety	Avoid	Council recognises that people are central to all of its operations and activities. Council seeks to avoid activities that expose staff, contractors, volunteers, residents, or visitors to unacceptable risks to their health, safety, or wellbeing. Council does not consider that a secondary risk appetite level is necessary for this Risk Category.
Reputation		
 Reputation	Avoid	Council has low (little-to-no) risk appetite for taking risk in the conduct of activities that are likely to result in widespread, irreparable or severe damage to Council's name. In the pursuit of its Strategies, Council seeks to Avoid adverse exposure to risks with regard to its reputation. However, in some circumstances Council may be willing to Accept risk relating to its reputation where there is a reasonable degree of protection.
Growth		
 Growth	Accept	With regard to Growth, Council is willing to ***Accept*** a medium level of risk in order to achieve its Strategies. Council will endeavour to select options based onoutcome delivery, whilst maintaining a reasonable degree of protection. Council does not consider that a secondary risk appetite level is necessaryfor this Risk Category

12. Risk Management Process

The Risk Management Process is the systematic application of management policies, procedures and practices to the tasks of establishing context, identifying, analysing, evaluating, treating, monitoring and communicating in relation to risk.

Council will apply the following Process as defined by *AS ISO 31000:2018 Risk Management - Guidelines*:



The Process will be undertaken and documented using Council's risk assessment templates and criteria.

Council's Risk Management Team will provide practical assistance to Council staff in completing and documenting each step of the process; however, a basic overview of the process is on the next page.

Risk Management Process Overview

Step 1	**Communication and Consultation**	Communication and consultation with relevant internal and external stakeholders is to be undertaken at all stages of the risk assessment process to bring different areas of expertise together, ensure different views are appropriately considered, provide sufficient information to facilitate risk oversight and decision making and to build a sense of inclusiveness and ownership among those affected by the risk. It involves promoting awareness and understanding, as well as seeking feedback and information to support decisions made throughout the process.
Step 2	**Establishing the scope, context and criteria**	This part of the process is undertaken to gain an understanding of the purpose of the risk assessment and factors that may require consideration throughout the process. It includes establishing and defining the scope of the activity being assessed and associated boundaries of the risk assessment; the relevant objectives to be considered and any relevant relationships to other projects, processes and activities; desired outcomes from the steps to be taken; decisions that need to be made; the internal and external environment; resources required and associated responsibilities; risk assessment criteria, tools and techniques to be applied and records to be kept throughout the risk assessment process.
Step 3	**Risk Assessment**	***The risk assessment process comprises the following key steps:***
	1. Risk Identification	Identifying risks involves consideration of what, how, why and when events might occur that could have an impact on achieving the objectives of the activity or operation being assessed. During this process consideration is to be given to Council's adopted **Risk Categories**. Relevant, appropriate and up to date information is important to identifying risks.
	2. Risk Analysis	Risk analysis is undertaken to determine and understand the level of risk being faced. It involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. Risk analysis provides input to risk evaluation, decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment and methods. Risk analysis should be undertaken using Council's adopted **Risk Assessment Criteria**.
	3. Risk Evaluation	The purpose of risk evaluation is to support decisions. It involves comparing the results of the risk analysis with the Council's established risk criteria to determine if the level of risk is acceptable or additional action is required in order to continue with the activity or operation being assessed. Options may be to do nothing; consider risk treatment options; undertake further analysis; maintain existing controls; reconsider objectives; and it should consider the wider context and the action and perceived consequences to both internal and external stakeholders.
Step 4	**Risk Treatment**	Risk Treatment involves the development and implementation of additional controls, such as systems and procedures, to address the risk. Risk Treatment involves an iterative process of formulating and selecting risk treatment options; planning and implementing risk treatment; assessing the effectiveness of the treatment; deciding on whether the remaining risk is acceptable and if not acceptable, taking further treatment. Depending on the activity or operation that is being assessed and the priority of the risk, risk treatment strategies can involve the development and implementation of long or short term risk treatment action plans. **Risk Evaluation (Step 3)** and **Risk Treatment (Step 4)** should be undertaken with consideration of Council's adopted risk appetite.
Step 5	**Monitoring and Review**	Monitoring and review of the risk management process, its implementation and outcomes ensures its continued quality and effectiveness and identifies opportunities for improvement. It will ensure that identified risks and controls remain relevant, controls remain effective and that any new risks are appropriately identified, recorded and managed appropriately. It should be a planned and documented part of each stage of the process and associated responsibilities should be clearly defined.
Step 6	**Recording and Reporting**	The risk management process and its outcomes are required to be documented and reported regularly to ensure continued communication in relation to risk management activities and outcomes, to provide information for decision-making, to improve risk management activities and to assist interaction with stakeholders.

13. Risk Assessment Form

To ensure a consistent approach to documenting risk, Council staff will document the risk assessment process using Council's standard Risk Assessment Form template. The level of detail recorded will be commensurate with the activity or project scope, level of risk and resource availability. Council's Risk Assessment Form is maintained by Council's Manager Governance & Risk.

14. Risk Assessment Criteria

The risk management process will be undertaken in accordance with Council's following adopted criteria to assess strategic and operational risks (unless exceptions below apply). The criteria are aligned with Council's organisational key objectives and risk appetite.

Table 1	**Risk Consequences Rating**	To determine the types and severity of risk consequences that could arise
Table 2	**Risk Likelihood Rating**	To determine how likely it is that the risk consequences will occur
Table 3	**Acceptability of Residual Risk**	To determine whether the level of risk remaining after treatment is within Council's defined risk appetite and tolerance, and whether it can be reasonably accepted
Table 4	**Risk Rating Matrix** *(risk rating calculation tool)*	Risk Rating = Consequence Rating x Likelihood Rating
Table 5	**Preferred Risk Treatment Options and ALARP**	To establish the preferred risk treatment option to manage the risk and determine whether escalation is necessary

Exceptions to risk assessment criteria

While risks are generally managed under Council's Risk Management Framework, some categories require tailored approaches due to their specialised nature or regulatory obligations.

Water and sewerage risks

All water and sewerage operational risk will be assessed in accordance with the criteria adopted in this Framework, or as necessary, in accordance with criteria that is specifically prescribed by external regulators (eg. the Australian Drinking Water Guidelines and Australian Guidelines for Water Recycling).

Work health & safety risks

Work health and safety risks at the higher strategic, divisional and operational level will be assessed in accordance with this Framework. However onsite operational WHS risks will be assessed in accordance with the procedures defined in Council's *Work Health & Safety Management System* and defined risk assessment criteria that aligns to this Framework.

Event Risks

Event risks will be assessed in accordance with the procedures defined in Statewide Mutal Event Management best practice Guidance Notes

Council's Risk Rating Matrix and Preferred Risk Treatment Options (ie. Table 5 in this Framework) will still apply to the assessment and evaluation of these risks. This approach aligns with Statewide Mutual and the key objective of applying these criteria is to substantiate methodology used should Council's decisions be called into question from a legal standpoint.

Table 1: Risk consequence rating

The following is a guide for determining consequence:

		Risk Categories Consequence Descriptors						
		Financial (includes events, incidents, projects and long-term costs and efficiencies)	**Legal and Governance** (includes compliance, regulation, obligations and any other exposures even if also considered in other categories)	**Asset and Infrastructure** (Includes damages, assets, infrastructure, repairs)	**Environmental** (includes noise, ecosystems, heritage, water, land, air...)	**People and Safety** (includes the public and work related)	**Reputational** (includes media, perception, political view, and public trust)	**Growth** (Includes the local economy, local community and local businesses)
Consequence Levels	**Catastrophic (5)**	> $500k	Cessation of Activities	Extensive, widespread or permanent damage to assets/ infrastructure. And unable to continue normal activities.	Irreversible long-term	Death, severe permanent disablement, or adverse health effect	Censure / Inquiry	Detrimental impact on the local economy.
	Major (4)	$100K - $500K	Successful Prosecution	Major disruption to activities. Critical loss or permanent damage to assets / infrastructure. Replacement of part of asset/ infrastructure.	Wide long-term	Hospitalisation, serious injuries resulting in long term absences and adverse health effect	High media	Major impact on the local economy. Serious public outcry.
	Moderate (3)	$50K - $100K	Enforceable undertaking or fine.	Moderate to significant damage or loss of assets/ infrastructure. Significant repairs may be required. Temporary disruption of activities.	Wide short term	Medical treatment required and/or some lost time	Moderate Media	Significant impact on the local economy and significant public criticism.
	Minor (2)	$10K - $50K	Compliance breach resulting in corrective action.	Minor loss or damage to assets/ infrastructure. Minimal disruption to activities and may be some repairs required.	Minor short term	Medical treatment required, No lost time	Minor Media	Minor impact on development of the local economy.
	Insignificant (1)	< $10K	Technical compliance breach with limited material impact.	Negligible damage to or minimal loss of assets/infrastructure. No impact on ability to undertake activities and no repairs required.	Incident not requiring intervention	First Aid injury, No lost time	Incident that does not receive any coverage	Insignificant impact on local economy, local community / business concern.

Table 2: Risk Likelihood Rating

Likelihood	Descriptor	Probability of Occurrence
Almost Certain (5)	Expected to occur in most circumstances	Within 1 Year
Likely (4)	Will probably occur in most circumstances	Within 2 Years
Possible (3)	Might occur at some time	Within 3 - 5 Years
Unlikely (2)	Could occur at some time	Within 10 - 20 Years
Rare (1)	May occur in exceptional circumstances	More than 20 Years

Table 3: Control Effectiveness Rating

Acceptability of Residual Risk			
Risk Rating	**Level**	**Acceptability**	**Required Actions**
23 - 25	**Very High**	**Intolerable**	Exposure to risk or circumstance is to be **immediately discontinued** except in extreme circumstances. Permission to continue exposure will be from the relevant director with as much risk management rigour as practicable unless dire operational needs preclude doing so.
16 - 22	**High**	**Conditionally Tolerable with continuous review**	Exposure to the risk or circumstance would normally be discontinued as soon as is reasonably practicable. Continued exposure would only be considered in exceptional circumstances, and the decision to do so would be made by the relevant manager or coordinator after due consideration. Any decision to continue exposure must be subject to continuous review.
7 - 15	**Medium**	**Tolerable with periodic review**	Exposure to the risk may continue provided it has been appropriately assessed, has been mitigated to as low as reasonably practical, and is subject to periodic review to ensure the risk does not increase.
1 - 6	**Low**	**Acceptable with periodic review**	Exposure to the risk is acceptable, but is subject to periodic review to ensure risk does not increase.

Table 4: Risk rating matrix

Risk Rating = Consequence Rating x Likelihood Rating

Likelihood						
	Almost Certain (5)	Medium (11)	High (16)	High (20)	Very High (23)	Very High (25)
	Likely (4)	Medium (7)	Medium (12)	High (17)	High (21)	Very High (24)
	Possible (3)	Low (4)	Medium (8)	Medium (13)	High (18)	High (22)
	Unlikely (2)	Low (2)	Low (5)	Medium (9)	Medium (14)	High (19)
	Rare (1)	Low (1)	Low (3)	Low (6)	Medium (10)	Medium (15)
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
		Consequence				

Table 5: Preferred Risk Treatment Options (including ALARP)

Residual Risk Rating	Preferred Risk Treatment Options	**Reporting / Escalation** Minimum reporting / escalation level for decision to cease activity, continue activity or take other necessary actions
Very High	**Preferred treatment options: Avoid** → Cease activity, process or task until further directed. → Requires immediate escalation and active management through additional and effective treatment measures to reduce risk before proceeding. → Detailed planning required in consultation with the to prepare a risk management plan.	**Director** (escalate Director GM as deemed necessary)
High	**Preferred Treatment Options: Avoid, Transfer or Mitigate** → Subject to discussions with Manager (and/or Director), consider ceasing activity, process or task temporarily to consider alternative options or review risk treatment strategies to enhance adequacy and effectiveness. → Consider implementation of additional or improved controls to reduce the risk → Continue to monitor control effectiveness.	**Manager** (escalate to Director as deemed necessary)
Medium	**Preferred Treatment Options: Mitigate or Accept** → Subject to discussions with Supervisor, Coordinator or Team Leader (and/or Manager), review risk treatment strategies to determine their adequacy and effectiveness. → Consider implementation of additional or improved controls to reduce the risk → Continue to monitor control effectiveness.	**Supervisor, Coordinator or Team Leader** (escalate to Manager as deemed necessary)
Low	**Preferred Treatment Options: Accept and identify corrective action** → Manage by existing routine procedures and work practices. → Continue to monitor control effectiveness.	**Responsible staff** (escalate as deemed necessary)

ALARP – As low as reasonably practicable

ALARP involves weighing the benefits and opportunities to be gained from managing the risk and continuing with the proposed activity against the effort, time and resources needed to control the risk.

When determining if additional treatment options should be implemented, consideration should be given to the level of risk that would remain if additional controls were implemented.

Unacceptable - where the cost or resource required to implement further risk treatment is grossly disproportionate to the risk control improvement gained, a decision should be made to cease the activity altogether or find an alternative course of action (except in cases where overriding factors mean there is no choice but to implement the identified additional control measures).

Acceptable - ALARP - *aim for this level of risk treatment* - where the cost, resources and effort required to implement additional risk treatment is acceptable and worthwhile given the risk control improvement gained and resulting benefits achieved from continuing with the activity, operation or project being assessed.

15. Records Management

Adequately recording the risk management process will:

- Ensure compliance with the State Records Act 1998 (NSW) and associated Council policies
- Ensure the integrity of the process and support good corporate governance practices by demonstrating due diligence
- Provide an audit trail and evidence of a structured approach to risk identification and analysis;
- Provide a record of why decisions were made, including to assist in the defence of claims brought against Council; and
- Facilitate risk management reviews and reporting.

Until Council's corporate systems are harmonised or other risk management systems become available, Council will utilise Excel and existing corporate record keeping systems to record risk assessments, risk registers and associated documents, as well as to monitor and report on risks.

16. Risk Registers

Council will develop and maintain organisational Risk Registers to:

- Ensure that all internal and external risks and opportunities have been captured so that Council has a current and comprehensive understanding of its risks, as well as assurance that risks are being managed within Council's risk appetite; and
- Allow for effective risk and control evaluation, analysis, treatment, monitoring and reporting.

Collaboratively the following Risk Registers will form Council's risk profile and will inform process improvement opportunities across the organisation.

Register Type	Responsibility
Strategic Risk Register	Council's Governance & Risk team will hold workshops at a directorate level and with the Executive Directors develop a Strategic Risk Register. The Executive Directors are responsible to adequately maintain, monitor, review and report on the Strategic Risk Register in accordance with the Review and Reporting Schedule included in this Framework.
Operational Risk Register	Council's Risk Management Team will hold workshops at a Management level to develop Operational Risk Registers for each Department. Each Manager is responsible to adequately maintain, monitor, review and report on their Operational Risk Register in accordance with the Review & Reporting Schedule included in this Framework.
Project / Activity Risk Register	Council staff are required to undertake and document risk assessments where considered necessary in relation to day-to-day activities, operations and specific projects and the like so as to ensure risks are adequately addressed. Council's Risk Management Team will assist with this process. Circumstances that may warrant the development of specific risk assessments may include, but are not limited to: ▪ At the planning stages and during Council managed projects, including construction projects and major events; ▪ Where a new process is planned or an existing process is being reviewed. ▪ Following a significant incident, near miss or the like. ▪ When required by Council policy or procedure. ▪ As deemed necessary for inclusion in reports to Council in relation to matters such as requests for additional significant funding allocations and high risk projects.

Risk Registers will be made available to the Audit, Risk & Improvement Committee as necessary.

17. Resources and Committees

Resource / Committee	Responsibilities
Audit, Risk & Improvement Committee (ARIC)	Council's Audit, Risk & Improvement Committee (ARIC) is an independent advisory Committee to Council to promote good governance and practice throughout the organisation. Its role is to monitor, review and advise the Council on matters of accountability and internal control affecting the operations of Council. The role and responsibilities of the Committee are governed by its adopted Charter which defines its purpose, composition, structure, authority, scope of activities and reporting requirements.
Internal Audit Function	The Internal Audit function provides independent and objective assurance that Council's governance, risk management, and internal control systems are effective. It evaluates how significant risks are identified and managed, ensures compliance with legislative and policy obligations, and recommends improvements to strengthen practices. Internal Audit supports accountability and transparency by embedding risk management into decision-making and service delivery, and reports directly to ARIC and on audit findings and risk insights
Manager Governance & Risk	The Manager Governance & Risk's role is to implement the Risk Management Framework and promote risk management throughout the organisation to build a positive and proactive risk aware culture.

18. Roles, Responsibilities and Accountability

All Council staff are responsible to ensure they take an active role in the management of risks relative to their area of operation in accordance with this Framework. Risk management responsibilities will be included in staff position descriptions and accountability will be monitored.

The risk management responsibilities at the various levels of the organisation are defined below.

Roles	Responsibilities
All Staff and Volunteers	All employees and volunteers are required to undertake risk management training, identify and manage risks in their area of operation and responsibility in accordance with this Framework and to report risk related incidents in a timely manner.
Council (Councillors)	Council is responsible to set the organisational risk appetite and recognise the need for risk management resources to support the achievement of risk management objectives. Council will appropriately consider risk management issues raised in reports and make informed decisions based on the associated risks and potential opportunities. Council will give due consideration to risk management reports from Council's Audit, Risk & Improvement Committee.
General Manager	The General Manager is ultimately responsible to ensure there is an adequate risk management system in place that is consistent with Council's business, ethical and professional standards. The General Manager is responsible to ensure the resources are available to effectively implement and maintain Council's Risk Management Framework.
Executive Directors	The Executive Directors are responsible to advise on Council's risk appetite; promote risk management across the organisation and ensure risk management is embedded in their area of operation. Executive Directors will ensure the allocation of appropriate resources for the implementation and maintenance of Council's Risk Management Framework and is responsible for the development, ongoing review and refinement of Council's Strategic Risk Register.
Managers and Coordinator	Managers, Coordinators and Team Leaders are responsible to manage risk in their respective areas of accountability and responsibility and supporting employees in identifying, managing and communicating risk. Managers are responsible for the development and ongoing review of Operational Risk Registers within their area of accountability in accordance with this Framework. Managers, Coordinators and Team Leaders are responsible for promoting risk management in support of an organisational risk aware culture.
Manager Governance & Risk	The Manger Governance & Risk is responsible for developing and maintaining risk management protocols, procedures and tools and for providing risk management training and support throughout the organisation. They are responsible for regular reporting to the Executive Directors concerning risk management activities and facilitating the development and review of risk registers across the organisation.

19. Review and Reporting Structure

Council's risk review and reporting structure will be implemented to assist in:

- Monitoring Council's performance in mitigating risks and seizing positive opportunities
- Informing decision making, identifying improvement opportunities and improving performance
- Ensuring changing circumstances are considered against risk priorities, and any additional risks are identified, documented and assessed appropriately
- Reviewing relevance and effectiveness of existing risk controls
- Measuring the success of Council's Risk Management Framework.

Review by Council's ARIC is considered essential in ensuring the independent and holistic review of Council's performance and to provide assurance to the General Manager and Council that risks are being appropriately managed.

Reviews and reports will be coordinated by Council's Risk Management Team in accordance with the following schedule; however, it is noted that additional and/or specific risk management reporting may be required from time to time.

At a minimum, reporting on risks and risk management initiatives will be undertaken in accordance with this Framework.

Risk Management Activities

At a minimum, quarterly reporting will be undertaken on Council's overall risk management activities to both Executive Directors and Council's Audit, Risk & Improvement Committee.

Strategic Risk Register

Council's Executive Directors are responsible to review Council's Strategic Risk Register.

The Strategic Risk Register will be reviewed on a minimum annual basis and as high-level risks emerge. Reviews will be reported to Council's Audit, Risk & Improvement Committee.

Operational Risk Registers

Managers are responsible for the review of Operational Risk Registers. Operational Risk Registers will be reviewed on a minimum bi-annual basis, and as high-level operational risks emerge. Reviews will be reported to Executive Directors and where required to Council's Audit, Risk & Improvement Committee.

Council Managers will include a review of operational risks, controls and associated risk treatment action plans on their team meeting agendas. This will facilitate a consultative approach to ensuring risks remain relevant, controls continue to be effective and that any new or emerging risks are identified and managed adequately.

Risk Management Framework

To ensure its continued effectiveness and relevance and to identify improvement opportunities and in accordance with the *Guidelines for Risk Management and Internal Audit for Local Government in NSW* an annual self-assessment of Council's Risk Management Framework will be undertaken. The results of the self-assessment will be reported to the Executive Directors and Council's Audit Risk & Improvement Committee.

Where significant amendments to the Framework are recommended, approval will be required by the Executive Directors and a report presented to Council.

20. Performance and Success Measures

A review of Council's performance will assist in identifying improvement opportunities in relation to this Framework and will be reported to the Executive Directors and Council's Audit, Risk & Improvement Committee.

Council's Manager Governance & Risk may use various methods to measure and report on the strengths and weaknesses of Council's performance, including:

- Organisational surveys to monitor risk management awareness and knowledge
- Statistics on staff participation in risk management training
- Analysis of data gathered from organisational risk reporting and internal audit results, as well as incident and claim statistics.

Annexure A - Definitions

The key risk management terminology used within the Framework is in accordance with *AS ISO 31000:2018 Risk Management - Guidelines* and *ISO Guide 73:2009 Risk Management - Vocabulary*. ISO also maintains a terminological database at the following address: http://www.iso.org/obp

Risk Term	Definition
ALARP	'As Low as Reasonably Practicable' - ALARP involves weighing the benefits and opportunities to be gained from managing the risk and continuing with the proposed activity against the effort, time and resources needed to control the risk.
Communication & Consultation	Continual and iterative processes that an organisation conducts to provide, share or obtain information, and to engage in dialogue with stakeholders regarding the management of risk.
Consequence	The outcome of an event. A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.
Control	Measure that maintains and/or modifies risk. Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.
Establishing The Context	Defining the external and internal parameters to be taken into account when managing risk and setting the scope and risk criteria for the risk management policy.
Event	Occurrence or change of a particular set of circumstances. An event can have one or more occurrences and can have several causes and several consequences. An event can be a risk source.
Exposure	Extent to which an organisation and/or stakeholder is subject to an event.
Hazard	Source of potential harm. Hazard can be a risk source.
Inherent Risk	The level of risk that exists prior to the implementation of risk control measures.
Level of risk (risk rating)	Magnitude of a risk or combination of risks, expressed in terms of the combination of consequence and their likelihood.
Likelihood	The chance of the risk happening.
Monitoring	Continual checking, supervising, critically observing or determining the status in order to identify changes from the performance level required or expected. Monitoring can be applied to a risk management framework, process, risk or control.
Residual Risk	The level of risk remaining after risk control measures have been taken.
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives. Review can be applied to a risk management framework, process, risk or control.
Risk	Risk is the effect of uncertainty on objectives, where an effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats. Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.
Risk Analysis	Process to comprehend the nature of risk and to determine the level of risk. Risk analysis provides the basis for risk evaluation and decisions about risk treatment and includes risk estimation.
Risk Appetite	The amount and type of risk that an organisation is willing to pursue or retain.
Risk Assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk Criteria	Terms of references against which significance of a risk is evaluated. Risk criteria are based on organisational objectives and external and internal context.
Risk Description	A structured statement of risk usually contains four elements, events, causes and consequences.
Risk Evaluation	Process comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation assists in the decision about risk treatment.

Risk Identification	The process of finding, recognising and describing risks. Risk identification involves the identification or risk sources, events, their causes and their potential consequences. Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders needs.
Risk Management	Coordinated activities to direct and control an organisation with regard to risk.
Risk Management Framework	A set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. The foundations include the policy, objectives, mandate and commitment to manage. The organisational arrangements include plans, relationships, accountabilities, resources, processes and activities. Risk management framework is embedded within the organisation's overall strategic and operational policies and practices.
Risk Management Plan	Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk. Components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities.
Risk Management Policy	Statement of the overall intentions and direction of an organisation related to risk management.
Risk Management Process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk.
Risk matrix	Tool for ranking and displaying risks by defining ranges.
Risk Owner	Is the person or entity with the accountability and authority to manage a risk
Risk Profile	Description of any set of risks. The set of risks can contain those that relate to the whole organisation, part of the organisation or as otherwise defined.
Risk Register	Record of information about identified risks. The term "risk log" is sometimes used instead of "risk register".
Risk Reporting	Form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management.
Risk Source	Element which alone, or in combination, has the potential to give rise to risk.
Risk Treatment	Is the process to modify a risk. Risk treatment options include: ▪ Reducing the risk by lowering the likelihood and/or consequences of the risk. ▪ Sharing elements of the risk with key stakeholders. ▪ Eliminating the risk by avoiding the risk or removing the risk source. ▪ Taking or increasing the risk in order to pursue an opportunity or retaining the risk by informed decision. Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction"
Stakeholder	A person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
Types of Risk	***Strategic Risks*** *Risks (either internal or external) which may impact upon the ability of the organisation to achieve its strategic objectives as set out in Council's Community Strategic Plan.* ***Operational Risks*** *Risks which may impact upon the ability to achieve day to day service delivery commitments.*