Enterprise Risk Management Policy

Policy title	Enterprise Risk Management Policy
Responsible manager(s)	Director Corporate & Community
Contact officer(s)	Manager Governance & Risk
Directorate	Corporate & Community
Approval date	25 September 2025
Strategic Focus Area	LE Leadership LE.1. Lead, govern, and regulate with integrity, fairness, transparency, and accountability. frameworks and all relevant legislative, strategies, risk management, procedures and service standards. LE.3. Ensure that the Council maintains responsible financial, employment and management practices.

Introduction

Risk is the effect (either positive or negative) of uncertainty on business objectives. Risk influences every aspect of the operations of Hilltops Council (Council) and by understanding the risks we face and managing them appropriately Council enhances its ability to make better decisions, safeguard assets, provide services to the community, and achieve organisational goals.

Purpose/Objective

The purpose of this policy is to express Council's commitment to implementing organisation-wide risk management principles, systems and processes that ensure the consistent, efficient, and effective assessment of risk in Hilltops Council planning, decision-making and operational processes.

The objective of this policy is to align effective risk management practices across Council within a common framework that can be clearly understood and applied by everyone engaged in Council business. Specifically, this Policy aims to:

- Articulate an integrated framework for managing enterprise risks;
- Detail duties and responsibilities for risk owners relating to ERM; and
- Define the minimum requirements for undertaking a risk assessment.

The implementation of this policy requires commitment and resources at all levels of Council's organisation; with risk management forming an integral part of the decision-making process.

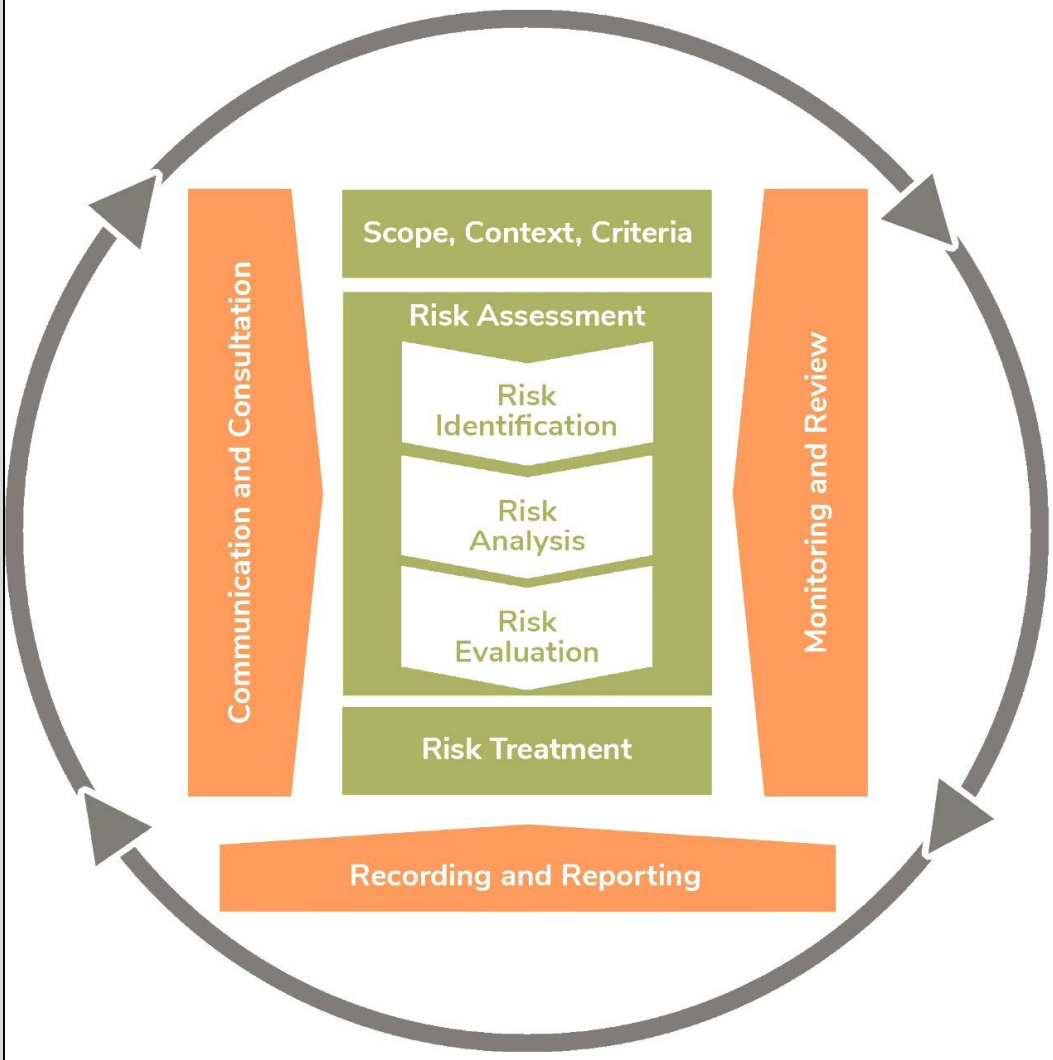
Policy Scope

Council is committed to managing risk on a systematic, organisation wide basis consistent with AS/NZS ISO 31000:2018. To achieve this requirement Council's Enterprise Risk Management (ERM) methodology applies to all Council staff and other key stakeholders who undertake activities on behalf of Council. To ensure the ongoing effectiveness of risk management within Council it is vital that ERM principles are integrated into the culture of the organisation. The General Manager, Executive Directors and Managers of Council are committed to the pro-active management of all risks in a systematic way to enhance our operational effectiveness.

Policy

1	**Roles and Responsibilities** Council aims to create a positive risk management culture where risk management is integrated into all everyday activities and managing risks is an integral part of governance, good management practice and decision-making at Council. It is the responsibility of every staff member and business area to observe and implement this policy and Hilltops Council risk management framework. All staff are responsible for identifying and managing risk within their work areas. Key responsibilities include: • Being familiar with, and understanding, the principles of risk management • Complying with all policies, procedures and practices relating to risk management • Alerting management to risks that exist within their area, and • Performing any risk management activities assigned to them as part of their daily role. Risk management is a core responsibility for all staff and management at Council. In addition to their responsibilities as staff members, Executive Directors and Managers are responsible for: • Ensuring all staff manage their risks within their own work areas. Risks should be anticipated, and reasonable protective measures taken • Encouraging openness and honesty in the reporting and escalation of risks • Ensuring all staff have the appropriate capability to perform their risk management roles • Reporting to the general manager/executive director on the status of risks and controls, and • Identifying and communicating improvements in hilltops council risk management practices to hilltops council risk management function. Council risk management function is available to support staff in undertaking their risk management activities. To ensure Council is effectively managing its risk and complying with its statutory obligations, Council's Audit, Risk and Improvement Committee (ARIC) and the Internal Audit function is responsible for periodically reviewing: • Risk management processes and procedures • Risk management strategies for major projects or undertakings • Control environment and insurance arrangements • Business continuity planning arrangements, and • Fraud control processes.
1.1	**Councillors** Councillors are not responsible for the day-to-day management of risk. Their role is to endorse Council's Risk Appetite Statement and to ensure that their decisions are consistent with the approved appetite. This provides strategic oversight and supports sound governance.
1.2	**General Manager** The General Manager is responsible for ensuring that risk is managed across all of Council's operations. Specifically, the General Manager will: • Promote the effective management of risk across the Council's operations • Ensure that Councillors are aware of risk management objectives • Ensuring the recognition and adoption of risk management as a key function of Council, and to ensure the inclusion of risk management as a priority within Council's Strategic and Operational Plans, Annual Report, and other appropriate Council documentation • Ensuring resources are appropriately allocated throughout the organisation to meet Council's risk management requirements.

1.3	**Executive Directors** Council's Executive Directors will: • Ensure all staff who report to them (either directly or indirectly) are fully conversant with and understand the role of risk management within Council operations • Ensure that there is adequate protection of Council's operations and assets from risk on an ongoing basis; considering appropriate budgeting, implementation of safety procedures, and loss-control programs • Support and encourage a risk aware culture within Council. • Be satisfied that all risks are appropriately identified, managed and controlled by each responsible risk owner within their directorate • Ensure that risk management is discussed at Executive meetings • Ensure that the Strategic Risk Register is review in accordance with the Risk Management Framework.
1.4	**Risk Owners (Relevant Managers, Coordinators and Supervisors)** Risk Owners are identified for all risks that are included in the risk registers. A Risk Owner is a senior staff member within an organisational unit, which is responsible, or should be responsible, for the management of the risk. Managers, Coordinators and Supervisors will: • Identify, assess and manage all their risks • Develop and implement risk management plans as appropriate for their risks using appropriate Council risk management templates • Allocate appropriate resources to effectively manage all identified enterprise risks • Lead and drive a positive risk culture within their section, areas or teams.
1.5	**Manager Governance & Risk** The Manager Governance & Risk will: • Facilitate risk management processes with all business units within Council • Provide regular reports on the status of Council's risk management to Executive Directors and ARIC. • Provide training and advice on risk management principles and processes • Develop and review risk management policies and procedures as required.
1.5	**Project Managers** In the context of risk management at Council a project manager is anyone working for Council that undertakes any project (for which they are responsible) that has the potential to impact (positively or adversely) on Council's strategic or operational goals. Project Managers will: • Ensure Council's Risk Management Policy and Framework is applied to the projects within their area of responsibility ensuring robust risk management controls are identified and implemented for their respective project • Undertake risk and opportunity assessments for all proposed projects in consultation with relevant stakeholders prior to the projects proceeding.
1.6	**Employees** Council Employees will: • Adhere to all corporate risk management requirements • Report risks (including loss or damage to council property) to their immediate supervisors.

3.	**Risk Management Process** Council risk management process is consistent with ISO 31000:2018 Risk Management Guidelines. The table below is adopted from this standard and depicts how risk will be managed at Hilltops: 
4.	**Risk Management Framework** Council has developed a Risk Management Framework to support the identification, treatment, monitoring, and review of risks to its operations and strategic objectives, ensuring appropriate internal controls are applied. The Framework aligns with the requirements of the OLG *Guidelines for Risk Management and Internal Audit for Local Government in NSW* and the principles of AS ISO 31000:2018 *Risk Management – Guidelines*. As a provider of essential services and infrastructure, and in meeting strategic obligations, Council must understand and manage internal and external risks that may impact service delivery and outcomes. The Risk Management Framework provides a structured approach to identifying, mitigating, and monitoring risks, supporting the efficient, effective, and ethical use of resources for the benefit of staff and the community The Hilltops Risk Management Framework is contained in a separate document.

6.	**Risk Assessment Requirements** While risk management is an ongoing activity, there are specific circumstances where the formal risk management process must be applied in accordance with Council's Risk Management Framework. These include: • Strategic Risks - The strategic risks will be reviewed on a minimum annual basis and as high-level risks emerge • Operational Risks – Risk assessments for routine activities and functions • Projects and Events – Risk assessments for individual projects and events delivered by Council.
7.	**Risk Appetite Statements** Risk appetite statements provide clear guidance on the level of risk an organisation is willing to accept in pursuit of its objectives. They support consistent decision-making by ensuring that risks are taken within defined and agreed boundaries. Council acknowledges that some level of risk is inherent in the delivery of services and achievement of strategic objectives. Council's risk appetite outlines the types and levels of risk it is willing to accept, with specific details set out in the Risk Management Framework.

Monitoring and Review

Council is committed to continually improving its ability to manage risk. Hilltops Council will review this policy and its risk management framework at least annually to ensure it continues to meet the requirements of the Local Government Act 1993, Local Government (General) Regulation 2021, and the Hilltops Council requirements.

Governance

This policy should be read in conjunction with any related legislation, codes of practice, relevant internal policies, and guidelines.

Related legislation and policies

Name	Link
Local Government Act (1993)	https://legislation.nsw.gov.au/
Risk Management Framework	Link TBD
NSW Office of Local Government (OLG) – Risk Management Guidelines for NSW Local Government	Guidelines for Risk Management and Internal Audit for Local Government in NSW
Procurement Policy	https://www.hilltops.nsw.gov.au/council/council-policies-plans/
Fraud and Corruption Policy	https://www.hilltops.nsw.gov.au/council/council-policies-plans/
Statement of Business Ethics	https://www.hilltops.nsw.gov.au/council/council-policies-plans/
Legislative Compliance Policy	https://www.hilltops.nsw.gov.au/council/council-policies-plans/

Legislative Frameworks Include

Name	Link
Work Health and Safety Act 2011	Work Health and Safety Act 2011 - NSW Legislation
State Records Act 1998	https://legislation.nsw.gov.au/view/html/inforce/current/act-1998-017
Privacy and Personal Information Protection Act 1998 (NSW)	Privacy and Personal Information Protection Act 1998 - NSW Legislation
Environmental Planning & Assessment Act 1979	https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1979-203
Swimming Pools Act 1992	https://legislation.nsw.gov.au/view/html/inforce/current/act-1992-049
Civil Liabilities Act 2002 (NSW)	https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2002-022
(NSW) Roads Act 1993	https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1993-033
Protection of the Environment Operations Act 1997	https://legislation.nsw.gov.au/view/html/inforce/current/act-1997-156
NSW Industrial Relations Act 1996	https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1996-017

Document History

Date	Status	Version	Resolution	Description
22 June 2022	Draft	0.1		Draft Enterprise Risk Management Policy presented to Council for 28 day public exhibition and submissions.
22 June 2022	Draft	0.2	22/128	Draft Enterprise Risk Management Policy Placed on 28 day public exhibition and submissions.
28 July 2022	Final	1.0	22/128	No submissions received after 28 day exhibition - Enterprise Risk Management Policy adopted
24 June 2025	Draft	1.1		Draft Policy was presented and reviewed by ARIC in accordance with the draft Risk Management Framework.
29 July 2025	Draft	1.2		Revised to include feedback from the ARIC
27 August 2025	Draft	1.3		Draft Enterprise Risk Management Policy presented to Council for 28 day public exhibition and submissions.
27 August 2025	Draft	1.4	22/255	Draft Enterprise Risk Management Policy Placed on 28 day public exhibition and submissions.
25 September 2025	Final	2.0	22/255	No submissions received after 28 day exhibition Enterprise Risk Management Policy - adopted

- This Enterprise Risk Management Policy shall be reviewed within 12 months of an election, and thereafter at intervals of no greater than four years. Any review will ensure this Policy continues to meet all statutory requirements and the operational needs of Hilltops Council. The Policy may also be reviewed at other times as determined by Hilltops Council .
- This Policy commences on and from the date of adoption by Hilltops Council as listed in the document history and replaces all previous versions.

Attachment 1 – Hilltops Risk Matrix and Descriptors

Hilltops Risk Matrix and Descriptors

The following risk matrix should be used by all sections and personnel within Council:

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				

The acceptability of residual risk table is used to explain required actions in relation to residual risks:

ACCEPTABILITY OF RESIDUAL RISK			
Risk Rating	**Level**	**Acceptability**	**Required Actions**
23 - 25	Very High	Intolerable	Exposure to rrisk 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.

The following table is to be used as a guide for determining likelihood:

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

The following is a guide for determining consequence:

				Risk Categories Consequence Descriptors				
		Financial (includes events, incidents, projects and long-term costs and efficiencies)	**Legal** (includes compliance, regulation, obligations and any other exposures even if also considered in other categories)	**Asset / Infrastructure** (Includes damages, assets, infrastructure, repairs)	**Environmental** (includes noise, ecosystems, heritage, water, land, air...)	**People – Health / 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.

Note: The table above is a guide for determining consequence as related to threats associated with a Council undertaking. It is acknowledged that the definition of risk articulated in the standard examines the effects of uncertainty on objectives which can include opportunity management. To assist Council staff a tool for determining opportunity is provided in the Risk Management Framework.