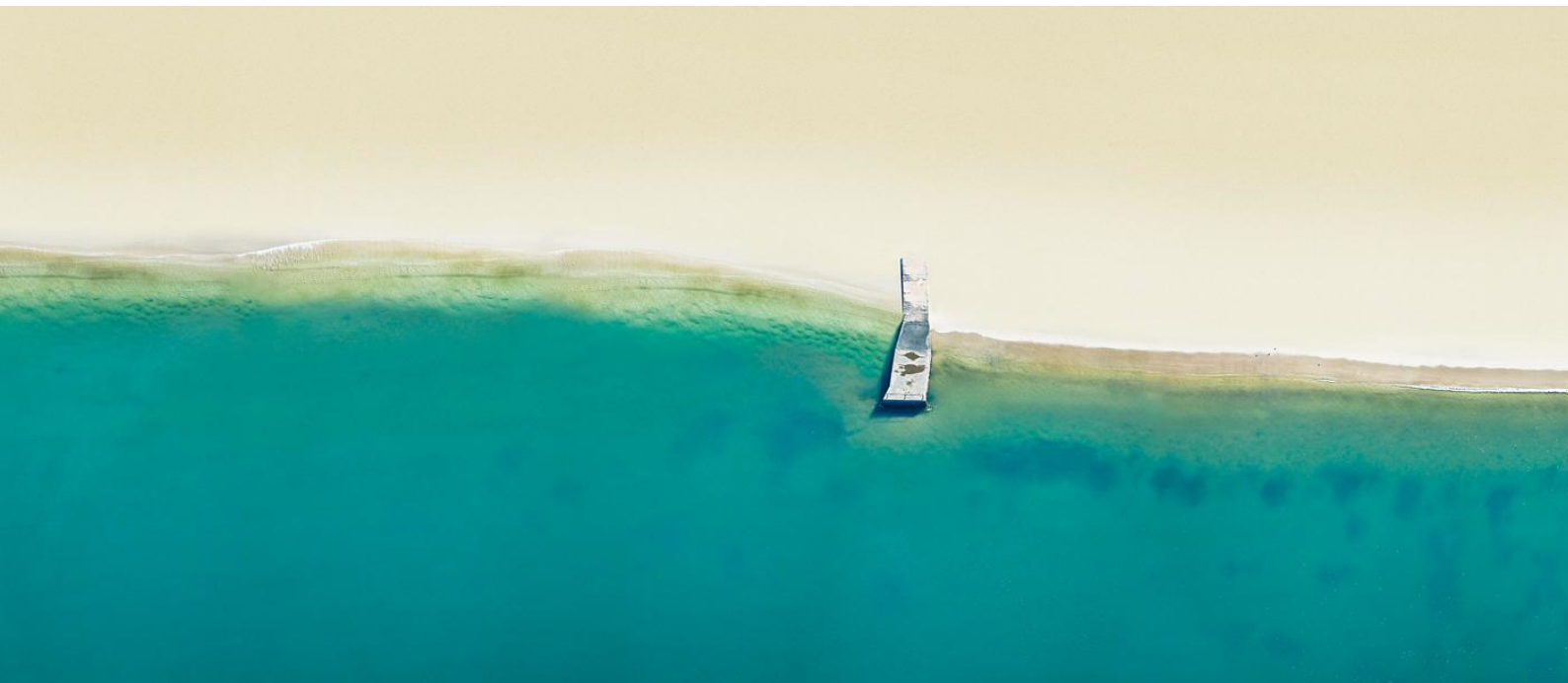
Bayside Council
Serving Our Community

Risk Management Procedure

5 November 2025



This procedure is structured in two distinct parts: Part 1 outlines the compliance formalities, and Part 2 provides the practical tools for risk assessment and management.

© Bayside Council

Risk Management Procedure
File: F13/418 Document: 17/42297 [v2]
Policy Register: F16/951 Policy No: PP19/9
Class of document: Corporate Procedure

Enquiries: Manager Governance and Risk

Telephone Interpreter Services - 131 450 Τηλεφωνικές Υπηρεσίες Διερμηνέων بخدمة الترجمة الهاتفية 電話傳譯服務處 Служба за преведување по телефон

Part 1 - The Formalities

What You Need to Know
Everyone plays a role in effectively managing material risks to Council. Each employee's level of responsibility depends on their job role and is described in this Framework. Risk management must be applied consistently across Council in accordance with this Framework and the procedural information contained within. Wherever we operate we will develop, implement and maintain management systems for all material risks that enable us to: • Identify, assess and manage risks in an effective and efficient manner; • Make decisions based on a comprehensive view of the reward-to-risk balance; • Provide greater certainty of the delivery of objectives; and • Satisfy our corporate governance requirements **This Procedure should always be read in conjunction with the related Policy.**

Purpose	This procedure ensures compliance with AS ISO 31000:2018, the Local Government Act 1993 (NSW), and NSW Office of Local Government (OLG) guidelines, providing a framework for identifying, assessing, and mitigating risks to achieve council priorities		
Scope	Councillors, Officers, Employees, Volunteers		
Related	Risk Management Policy		
Procedure Sections	Part 2 – Risk Assessment Tools How We Do Risk Management (link) Likelihood and Consequence Tables		
Compliance Requirements	Local Government Act 1993 NSW Local Government (General) Regulation 2021 NSW Office of Local Government Guidelines for Risk Management and Internal Audit for Local Government in NSW.		
Policy Owner	Manager Governance and Risk		
Effective Date	5 November 2025	**Review Date:**	5 November 2028

1 Risk Management at Council

Risk management refers to all of the actions that we take to reduce our exposure to risk to achieve our priorities. Risk management is an ongoing, proactive process that is part of a culture of continuous improvement. Risk management is integrated into day-to-day activities and informs all aspects of our business.

2 Roles and Responsibilities

Role	Responsibility
All Employees	• Understand Council's approach to risk management as set out in this procedure and Council's Risk Management Policy. • Identify, escalate, manage and report risk as part of day-to-day activities.
All Council Leads/ Co-ordinators and Supervisors	• Understand Council's Risk Appetite Statement Policy and apply the Risk Appetite Statement in decision making. • Actively identify, assess and treat risks within Council. • Ensure identified risks are recorded in Council's risk register. • Report and escalate high and significant risks to their Manager. • Report and escalate incidents to their Manager. • Where assigned as a risk owner, oversee implementation and effectiveness of risk controls and action plans. • Where assigned as an action owner, ensure actions are completed within the designated timeframe.
Council Managers	• Ensure employees are aware of and actively applying Council's approach to risk management. • Ensure Council's risk management procedure is integrated into planning, reviewing, reporting processes and project management. • Ensure decisions are made within Council's Risk Appetite. • Escalate high and significant risks, and activities outside of Council's Risk Appetite to the Executive Committee. • Prepare and implement action plans to treat risks outside of risk tolerance. • Regularly review the status and risk rating of identified risks. • Report incidents (risk events) and Key Risk Indicators as required by the Executive Committee.

Role	Responsibility
Executive Committee	• Ensure that all material risks within their business unit/shared service function are identified and managed effectively. • Ensure Council operates within Council's Risk Appetite. • Ensure that Council manages risk in an integrated and holistic manner.
Work & Health Safety / and Governance and Risk Team	• Oversee the implementation of Council's Risk Management Framework, policy, procedure and system. • Provide guidance on risk management within Council. • Coordinate risk reporting to the Executive Committee, the Audit Risk & Improvement Committee, and Councillors. • Provide ongoing employee awareness training and support materials to ensure all employees are aware of Council's approach to managing risk. • Ensure that Council's Risk Appetite is reflected in Council's policies.
Audit, Risk and Improvement Committee	ARIC advise the General Manager on key aspects of the risk management framework to ensure its adequacy, effectiveness, and alignment with council objectives. Key high-level responsibilities include: • Assessing the framework's overall structure, resources, consistency with Australian standards, integration across council operations, and quality of risk reports, plans, and delegations. • Evaluating risk culture, ethical commitments, staff training, leadership support, and impacts on insurance, asset management, and business continuity arrangements.
Executive Committee and Council	• Oversight of Council's risk management framework • Set, review and update Council's Risk Appetite.

3 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
- 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

4 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:

- 'Setting the tone at the top' - 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 Council's Insurance providers Continuous Risk Improvement Audits and risk initiatives.
- Ensure risks are escalated to the ARIC as per OLG circular

5 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 Risk Management team and Learning and Development 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

6 Types of Risk

This document deals with the following types of risk:

6.1 Strategic Risks

Threats and uncertainties that could affect the achievement of Council's strategic objectives. These risks arise from factors within the organisation's control (e.g. operational inefficiencies, succession planning, resource constraints) and external factors beyond its influence (e.g. regulatory changes, economic instability, community expectations, social dynamics)

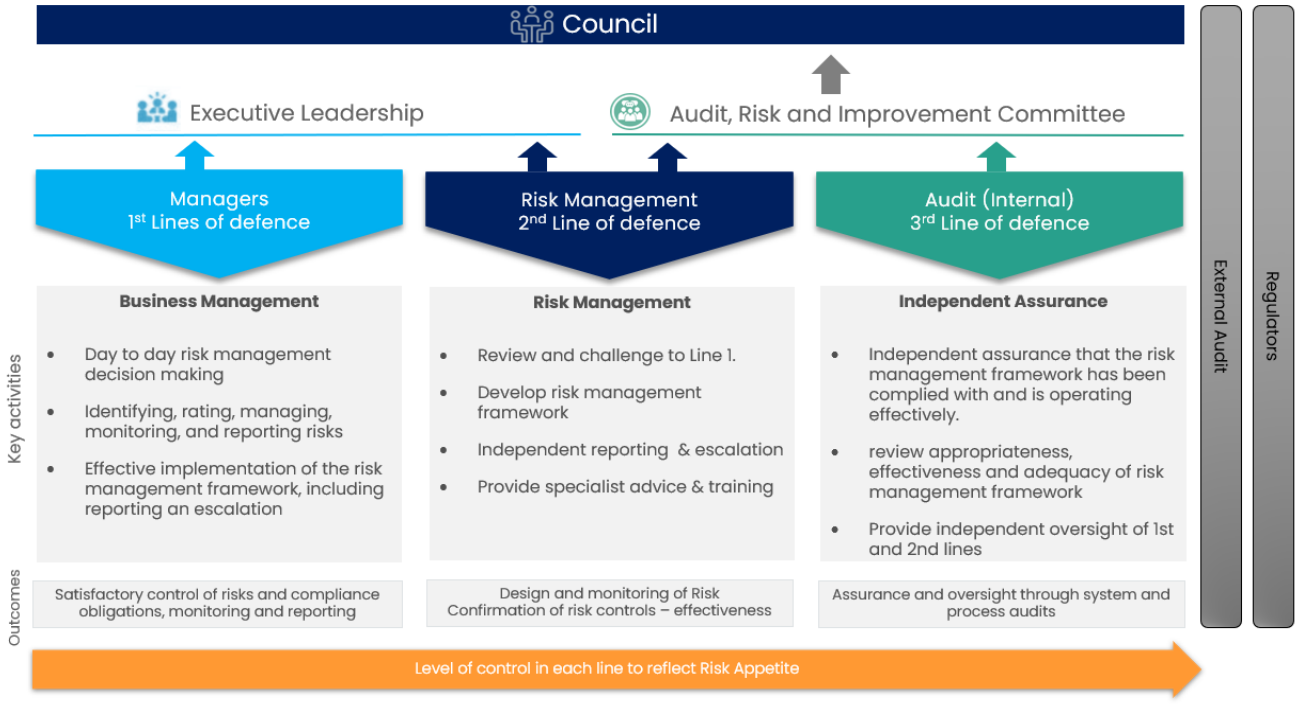
6.2 Operational Risks

Threats and uncertainties inherent in the day-to-day activities Council performs when delivering its services and functions

6.3 Project Risks

Threats and uncertainties that could affect the delivery of a project.

7 The Lines of Defence



7.1 First line of Defence (Operational)

Managers & risk owners use this framework to identify, assess, and manage risks and incorporate risk management in their daily activities and processes.

7.2 Second Line of Defence (Risk Management)

Council's Governance and Risk, Business Transformation including WHS and Information Technology teams provide compliant systems to support operations, as well as independent oversight and guidance on risk management activities.

7.3 Third Line of Defence (Internal Audit)

Internal audit periodically evaluates the Risk Management Framework to provide a level of assurance to senior management regarding the effectiveness of risk controls on a test basis and assessing whether the organisations risk management processes are reliable.

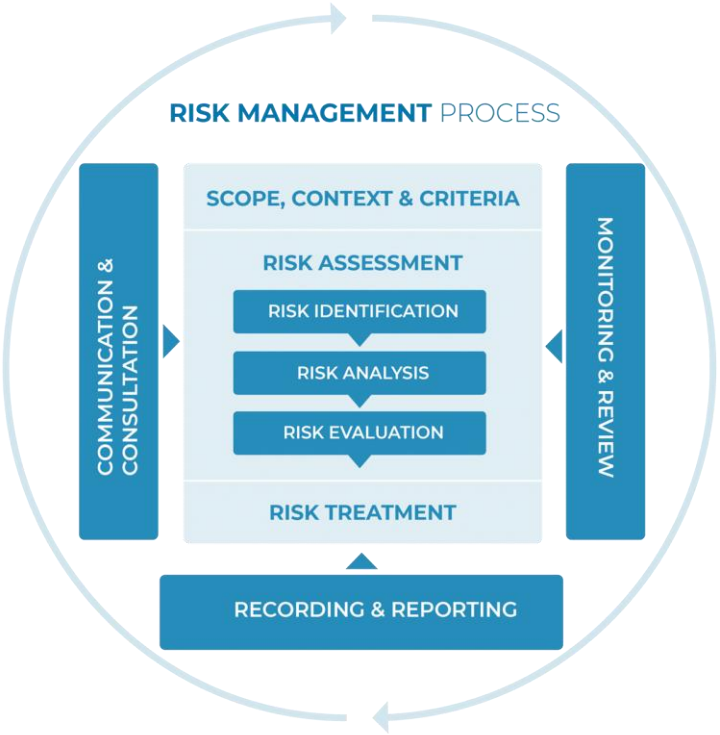
8 When a risk assessment is required

Risks should be assessed and reviewed whenever it is necessary. In addition, the following events should prompt consideration of the need for a risk assessment:

Strategic Planning	Risk assessments should be conducted during the strategic planning process to identify and assess strategic risks that may impact Council's objectives, priorities, and long-term sustainability. Changes in legislation.
Operational Planning	Risk assessments should be integrated into operational planning processes to identify and assess risks associated with day-to-day activities and service delivery. This helps prioritise risk management efforts and allocate resources effectively.
Project Lifecycle	Risks should be reviewed at each project phase, as outlined in Council's Project Management Framework, and reassessed if there are any substantial changes to projects.
Change Management	Risk assessments are integral to identifying potential risks that may arise from change to configuration of systems, equipment, or business processes.
Policy Development	When developing or revising policies, risk assessments should be conducted to identify and assess risks associated with policy implementation and compliance.
Incident Management	Following significant incidents or adverse events, risk assessments should be performed to analyse the root causes, assess the impact on Council, and identify preventive measures to mitigate against similar events occurring in the future. A risk assessment to identify potential hazards and prevent future incidents should be performed following a 'near miss'.

9 Our Risk Assessment Process

Councils risk assessment process follows the standard risk management process consistent with ISO 31000:2018 *(or as updated)*



10 RISK REGISTER

Risk registers provide managers with a list of identified risks that are clearly stated and assessed as to their importance to meeting Bayside's objectives.

Risks are to be captured in our risk System Pulse (refer Section 11).

The relevant manager for each area, project or is responsible for identifying, reviewing and responding to risks.

11 OUR RISK SYSTEM (PULSE)

Process for Risk Register entry and review process

Identified risks are to be entered into the Pulse system in the Risk Register.

Part 2 – The Tools

This section provides practical tools for assessing and managing risks.

HOW WE DO RISK MANAGEMENT

The Risk Team can provide guidance on this process.

STEP	WHAT WE DO	WHY WE DO IT	HOW WE DO IT
A	**Establish our Risk Environment** Start by identifying your objectives within Bayside 's risk environment. In establishing the context, consideration should be given to: • Start by defining the objectives your project/ business unit/ activity is setting out to achieve • Consider what internal and external factors/ threats exist that might impact your ability to achieve those of objectives • Consider, are there other opportunities that arise because the threat exists? • Identify the strengths and weaknesses of our operations relevant to the project/ business unit/ activity • identify relevant stakeholders • Understand the regulatory environment in which you are operating.	• To understand what may influence our ability to achieve our strategic objectives • To identify opportunities that might exist within our risk environment that can be explored.	• Strength, Weakness, Opportunity and Threat analysis (SWOT). • Other methodologies also look at Political factors, economical factors, social factors, technological factors, ethical factors and legal/ compliance factors.
B	**Identify the Risk** The aim of risk identification is to develop: • A comprehensive list of threats and opportunities based on events that might enhance, prevent, degrade, accelerate or delay achieving Bayside 's outcomes. • Provide information about risks so that we can analyse, evaluate, treat, monitor and report on them • identifying a responsible owner for managing risk	• To identify and understand what might inhibit the ability to meet objectives (ie what could go wrong) • To identify and understand what might cause these events to occur • To identify what controls we may have in place that are aimed at reducing the likelihood of the risk event happening in the first place, and if they do happen, what we have in place to reduce their impact (consequence).	• Think about all the things that could go wrong. • Engage with other areas of the business and shared service. Everyone brings a different perspective to the identification of risk. • Hold a risk workshop. The Risk Team can help you facilitate a workshop. Refer to Section **11 Our System** below
C	**Analyse the Risk** To analyse risks, develop an understanding of the risk and how it may impact Bayside. This is expressed in terms of the consequence and likelihood of the risk occurring: • consequence – considers what could happen if the risk was realised • likelihood – considers the probability of the risk will be realised. We assess risks at two points: **Current Risk:** This is the risk as it exists at the time of identification. It takes into account the controls that exist at the time. **Target Risk:** This is the risk you are aiming for after you have put in place actions to mitigate the risk (refer to section E below).	• Analysing risk ensures that we focus our attention on those risks that have the most severe consequences or have the greatest likelihood of occurring. • Understanding both the consequence and likelihood of risk occurring determines the action that we take to manage the risk. • By using a consistent methodology to analyse risks, we ensure we have a consistent understanding of risk across Bayside.	The first step is to categorise the type of risk (e.g. financial risk, regulatory risk, service delivery risk etc.). A risk will often involve multiple categories. Where this occurs, categorise the risk by the most predominate category. *Refer to Section Information on how to identify and describe risks on our Intranet.* The second step is to analyse the consequences, should the risk eventuate, and the likelihood that the risk will eventuate. *Refer to Section Information on Bayside 's risk categories.on our Intranet* The third step is to determine the risk rating using Bayside Risk Matrix *Refer Section Bayside 's consequence and likelihood ratings on our Intranet* Refer to Section **11 Our System** below
D	**Evaluate the Risk** To evaluate the risk you need to: • Combine the consequence and likelihood assessment, using Bayside 's risk matrix to determine the risk rating. • Consider whether the risk, as rated, is the risk within the tolerances set out in Council's Risk Appetite (our Willingness to accept)	• Understanding the risk rating and whether it is within Buyside's Risk Appetite determines the extent to which we need to respond and the urgency of our response.	Use your consequence and likelihood ratings to determine the risk rating *Refer information on Bayside 's Risk Matrix on our Intranet* Assess the risk rating against the appropriate risk category within the Risk Appetite – Our Willingness to Accept to determine whether the risk is within Bayside 's tolerance. *Refer to the Bayside Risk Appetite* Refer to Section **11 Our System** below
E	**Respond to the Risk** Following the guidance in section D (Evaluate the Risk) you now need to respond to the risk. Your response options are: • Avoid the risk: by deciding not to proceed or continue with the activity or choosing an alternative approach to achieve the same outcome. The aim is risk management, not aversion.	• To ensure that Bayside is a sustainable organization providing positive outcomes for its customers, we must appropriately and adequately respond to risk. • If we fail to respond to risk, we may place the wellbeing of our customers, employees and Bayside in danger.	Document how we are intending to respond to identified risks. *Refer to attachment X for information on responding to risks* How quickly we respond to the risk and the urgency of actions is determined by the risk rating (step D). • For risks rated **Extreme** – Requires immediate escalation and active management through additional and effective treatment measures to reduce risk before proceeding. Detailed planning required in consultation with the General Manger (GM) to prepare a risk management plan • For risks rated **High** – Subject to discussions with Manager (and/or Director), consider ceasing activity,

STEP	WHAT WE DO	WHY WE DO IT	HOW WE DO IT
	• Mitigate: Reduce the likelihood by improving management controls and procedures. Reduce the consequence by putting in place strategies to minimise adverse consequences, e.g. contingency planning, Business Continuity Plan, liability cover in contracts. • Transfer the risk: Shifting responsibility for a risk to another party by contract or insurance. It can be transferred as a whole or shared. • Accept the risk: Controls are deemed appropriate. They must be monitored and contingency plans developed where appropriate		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 • For risks rated **Medium** – Subject to discussions with Supervisor, Co-ordinator or Team Leader (and/or Manager), review risk treatment strategies to determine their adequacy and effectiveness. You must implement your response to risk within a few months. • For risks rated **Low** – you should prioritise to address as and when is reasonable, ensuring that higher rated risks are prioritised. Refer to Section **11 Our System**
F	**Reevaluate target risk level** Taking into account your response to the risk complete steps C to D again to determine: • Your target risk rating • Whether you are now operating within Bayside 's Risk Appetite	If are target risk is not within Bayside 's Risk Appetite, it means we need to take more action to respond to the risk, or we should not be doing the activity that gives rise to the risk.	
G	**Control Self-Assessment (CSA)** We should continuously assess identified risks and the effectiveness of the controls mitigating those risks. To achieve this, we implement CSAs to clarify business objectives and to identify and deal with the risks to achieving those objectives. This creates a clear line of accountability for controls, and a reinforced governance regime. **The Risk Team will assist with Control Self Assessments**	**12** The process of completing CSAs improve the internal control environment of an organisation by: • Increasing awareness of organisational objectives and the role of internal control in achieving goals and objectives • Motivating personnel to carefully design and implement control processes and continually improve operating control processes • A well-designed CSA helps management to reduce the costs of oversight activities while expanding their coverage	This will be managed through our risk management system PULSEn Refer to Section **11 Our System**

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 Impact / 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 will occur
Table 3	Control Effectiveness Rating	To calculate the effectiveness of controls on reducing the likelihood and consequences of the risk
Table 4	Risk Rating Matri (risk rating calculation tool)	To calculate the overall Inherent Risk Rating (prior to controls) and Residual Risk Rating (after controls); Risk Rating = Consequence Rating x Likelihood Rating
Table 5	Preferred Risk Treatment Options	To establish the preferred risk treatment option to manage the risk and determine whether escalation is necessary

Table1: Impact/ Consequence Rating Table

If this risk was to eventuate (i.e. become and event/incident) it could result in

Risk Categories What could be the consequences if the risk occurs?		Consequence *If you are unsure of the rating description refer to table 1.a)*				
		Insignificant 1	**Minor 2**	**Moderate 3**	**Major 4**	**Severe 5**
Financial	Risks that have a financial impact on the Council (revenue, expenses, assets, liabilities, reserve)	Negligible financial Loss relative to the circumstances: **Recurrent impact** <$50K **One off Impact** <$250K	Minor financial loss relative to the circumstances *(not covered by insurance)* **Recurrent Impact** $50K - $250K **One off Impact** $250K - $500K	Significant financial loss relative to the circumstances *(not covered by insurance)* **Recurrent Impact** $250K - $500K **One off Impact** $500k - $2M	Major financial loss relative to the circumstances (not covered by insurance) **Recurrent Impact** $500k - $3M **One off Impact** $2M – $20M	Extensive financial loss relative to the circumstances (not covered by insurance) **Recurrent Impact** >$3M **One off Impact** >$20M
People, Safety and Wellbeing	Risks that impact the health and safety of staff, as well as contractors & volunteers	**Physical (Staff/Public):** Minor injuries or illness treated at the scene. **Psychosocial:** Temporary low morale or minor dissatisfaction; no measurable impact, resolved internally.	**Physical (Staff/Public):** Injuries requiring medical attention but with no lasting effects. **Psychosocial:** Isolated complaints (e.g., stress, minor bullying); slight absenteeism; resolved internally, no external reporting.	**Physical (Staff):** One permanent disability or hospitalisation of multiple staff with injuries lasting 6+ months, where Bayside is mainly responsible. **Physical (Public):** One permanent disability or hospitalisation of multiple public members due to an incident where Bayside is at fault or contributed. **Psychosocial:** Widespread complaints (e.g., bullying, stress); moderate absenteeism or minor turnover; requires internal or external intervention.	**Physical (Staff/Public):** One death or multiple permanent disabilities due to an incident where Bayside is mainly responsible or at fault. **Psychosocial:** Significant culture issues (e.g., systemic bullying/stress); high absenteeism or turnover; requires external mediation or regulatory action (e.g., SafeWork NSW notice).	**Physical (Staff/Public):** Multiple deaths or permanent disabilities due to an incident where Bayside is mainly responsible or at fault. **Psychosocial:** Critical wellbeing crisis; mass turnover, staff shortages, widespread hazards (e.g., burnout, harassment); potential prosecution or class action; long-term cultural reform needed.
	Risks that impact the health and safety of the community	Insignificant injury: no medical treatment required	Short term isolated incidents of illness or injury; first aid required	Medium term illness or injury; medical attention required; health impacts in single Council locality *(Insurers require notification)*	Long term illness or injury: long term medical attention required; health impacts in multiple Council localities *(Insurers require notification)*	Fatality; permanent disability; illness or disease; widespread health impacts across LGA *(Insurers require notification)*
Service Delivery (based on Key Essential Services)	Risks that impact the ability to deliver internal and external services	Minor scheduled or unscheduled service disruption lasting less than 1 day (e.g., short delay in waste collection or brief interruption to community facilities). No impact on community safety or Council objectives.	Unscheduled service disruption lasting **1 – 3** days (e.g., delayed waste collection, temporary closure of a community facility such as a public pool or library). Minimal resource reallocation, Council objectives still met; limited community complaints.	Service disruption lasting **3–14** days (e.g., temporary shutdown of a public water refill station due to bacterial contamination, significant waste delays, or major road inaccessibility). Partial failure to meet Council objectives; moderate community disruption.	Prolonged service disruption lasting **2–4 weeks** (e.g., Extended closure of a public toilet blocks due to structural damage or blocked sewer lines., or critical road network failure). Multiple Council objectives unmet; significant community impact	Critical service failure lasting more than **1 month** (e.g., Long-term closure of key transport corridors servicing Sydney Airport due to major infrastructure collapse, causing widespread travel disruption and economic impact. complete breakdown of waste systems). Most Council objectives unmet; serious health/safety risks; potential OLG intervention; long-term loss of community trust.
Regulatory	Risks arising from non-compliance with legislation, regulations, or council policies, including breaches of laws governing council operations, safety, environment, and integrity. If this risk eventuates, it may result in legal action, fines, enforceable undertakings, or reputational damage.	Minor non-compliance with no external action. Technical breach resolved internally.	Minor breach of legislation or policy resulting in warnings or improvement notices (e.g., from SafeWork NSW).	Breach leading to external investigation or audit with negative findings. Fines or penalties issued under legislation such as the WHS Act 2011 or EPA Act 1979.	Serious breach resulting in formal enforcement action or adverse findings. Investigation by external agency (e.g., ICAC, SafeWork NSW) with reputational or financial consequences.	Significant breach resulting in prosecution, council dismissal, or state intervention. ICAC investigation or breach of the Local Government Act 1993. Maximum fine imposed on Council or an officer; potential criminal prosecution of an officer.
Reputation	Risks that impact Council's reputation in the community and media, as well as with the government	Isolated complaints from members of the community; one off insignificant enquiries from local media and/or on social media	Minor unfavourable local and/or social media attention; heightened concern and criticism from narrow group/s within the community	Short-term adverse local and / or social media attention; moderate community dissatisfaction; potential government agency concern	Significant adverse local / state media attention; public outcry and community dissatisfaction across multiple Council localities; potential government agency enquiry	Sustained adverse local, state and/or national media attention; severe widespread dissatisfaction and loss of community trust; potential loss of Government support & adverse intervention
Environment	Risks that impact the natural environment	Minor effects on the built or natural environment. Breach of guidelines or perceived damage with no lasting impact.	Short-term effects on the built or natural environment. Damage to a single property or parcel of land. Breach of council policy or environmental standards.	Serious medium-term environmental impact from a single incident (e.g., one-off pollution spill). Requires remediation or regulatory reporting.	Significant long-term impact on the built or natural environment. External investigation with adverse findings (e.g., EPA or planning authority).	Very serious or irreversible damage to the environment. Impact across multiple sites or ecosystems. Prosecution of Council or enforceable undertakings issued by a regulator.
Information / Cyber Security	**Information Management** Risks that impact the confidentiality, integrity, and availability of information	No exposure	Minor non-critical data exposure, quick fix, low cost.	Moderate data exposure, reportable breach, moderate cost/fines.	Significant data exposure, major disruption, high cost/fines.	Extensive data exposure, severe disruption, extreme cost/fines. Access to Personally Identifiable Information and or Protected Health Information
	Non – Critical and Critical Systems Risks that impact the integrity, and availability systems.	**Non-Critical Systems**: No impact. **Critical Systems**: No impact.	**Non-Critical Systems**: Minor issues, quick fix, low cost. **Critical Systems**: Minor issues, quick fix, low cost	**Non-Critical Systems**: Moderate degradation, some impact, moderate cost. **Critical Systems**: Moderate degradation, some impact, moderate cost.	**Non-Critical Systems**: Major disruption, high cost, media attention. **Critical Systems**: Significant downtime, high cost	**Non-Critical Systems**: Severe disruption, extreme cost, loss of trust. **Critical Systems**: Complete failure, critical operations halted, critical cost
Project Deliverables	**Budget** Risks that impact the ability to deliver project outcomes within budget	Minimal budget variance can be absorbed within contingency. No impact on project progress or council services	Minor budget overrun; requires reallocation, no impact on delivery	Noticeable budget overrun; requires approval for additional funds, some impact on delivery	Major budget overrun; significant impact on delivery, requires project scope reduction or major funding approval	Severe budget overrun; project cannot be completed, funding withdrawn, contract termination, legal or reputational consequences
	Timeframe Risks that impact the ability to deliver project outcomes within timeframe	Negligible delay; no impact on milestones	Minor delay; milestones adjusted, no impact on overall delivery	Moderate delay; some milestones missed, moderate impact on stakeholders	Major delay; critical milestones missed, significant stakeholder impact, possible penalties	Severe delay; project fails to deliver, contract termination, legal or reputational consequences
Strategic	Risks that impact long-term council objectives, such as community plans, policy implementation, or governance	Minor deviation from strategic goals; no long-term effect, easily corrected	Short-term setback in one objective; minor policy adjustment needed	Moderate impact on multiple objectives; requires resource reallocation, delays in community plan delivery	Significant failure in key strategic areas; major policy revisions, loss of partnerships or funding	Strategic failure; inability to achieve core community outcomes, potential council restructuring or intervention by OLG

Table 2: Risk Likelihood

The risk analysis process uses assessments of likelihood and consequence to determine the level of risk by reference to the risk matrix below.

'Likelihood' is a qualitative assessment of the frequency or probability of the identified risk occurring by reference to the following descriptors:

Likelihood Rating		Description	Operational Frequency
Almost Certain	**5**	This event is expected to occur in most circumstances	More than once per year ***or*** incident is clearly imminent
Likely	**4**	This event will probably occur in most circumstances	At least once per year
Possible	**3**	This event should occur at some time	At least once in 5 years
Unlikely	**2**	This event could occur at some time	At least once in 20 years
Rare	**1**	This event may only occur in exceptional circumstances	Less than once in 50 years

Consequence refers to the potential impact or magnitude of a risk, assessed using the descriptors provided in Table 1. To ensure accuracy and consistency, it is important to identify the 'worst credible outcome' that could result if the risk were to occur, rather than the 'worst possible outcome.

Table 3: Control effectiveness rating

Control Effectiveness Rating		Description	Operational Application
CONTROL STRENGTH	**Not Effective**	Significant control gaps that result in the control not influencing the risk level	At best, control addresses risk, but is not documented or in operation; at worst, control does not address risk and is neither documented nor in operation
	Partially Effective	Some control gaps that result in the control having limited influence on risk level	Control addresses risk at least partly, but is not documented and/or operation of control needs to be improved
	Moderately Effective	Fe control gaps. The control is influencing the risk level however, improvement is needed	Control addresses risk but documentation and/or operation of control could be improved
	Effective	No Control gaps. The control is influencing the risk level and only continued monitoring is needed	Control addresses risk, is officially documented, in operation and has been tested to confirm effectiveness

Table 4: Risk rating matrix

The intersection of likelihood and consequence on the matrix determines the level of risk. For example, a risk with a 'Likelihood' of Almost Certain and a 'Consequence' of Moderate gives a risk rating level of High.

		Risk Likelihood Rating				
Risk Consequence Rating		Rare	Unlikely	Possible	Likely	Almost Certain
		1	2	3	4	5
Severe	5	Medium (5)	High (10)	High (15)	Extreme (20)	Extreme (25)
Major	4	Low (4)	Medium (8)	High (12)	High (16)	Extreme (20)
Moderate	3	Low (3)	Medium (6)	Medium (9)	High (12)	High (15)
Minor	2	Low (2)	Low (4)	Medium (6)	Medium (8)	High (10)
Insignificant	1	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)

Risk Rating = Consequence Rating x Likelihood Rating

By assessing the level of risk from both an inherent (before controls) and a residual (after controls) perspective, the effectiveness of risk controls is demonstrated.

Table 5: Risk Treatment Options

When a risk level that is above appetite has not been accepted by the General Manager or relevant Director, a risk treatment plan must be initiated by the risk owner and monitored until resolved. How the risk in question proceeds whilst treatment is underway is at the discretion of the relevant Director or General Manager.

Treatment options include avoiding the risk, eliminating the source, or modifying the risk likelihood or consequence through the implementation of additional controls

Evaluated Risk Rating	Preferred Risk Treatment Options	**Reporting / Escalation** Minimum reporting / escalation level for decision to cease activity, continue activity or take other necessary actions
Extreme	**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 Director (GM) to prepare a risk management plan.	**General Manager** (escalate Council as deemed necessary, Critical Incident formation as directed by GM as 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, Co-ordinator 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, Co-ordinator or Team Leader** (escalate to Manager as deemed necessary)
Low	**Preferred Treatment Options: Accept and identify corrective action** • Manage by existing routing procedures and work practices. • Continue to monitor control effectiveness.	**Responsible staff** (escalate as deemed necessary)

- For risks rated **Extreme** – Requires immediate escalation and active management through additional and effective treatment measures to reduce risk before proceeding. Detailed planning required in consultation with the General Manger (GM) to prepare a risk management plan
- For risks rated **High** – 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
- For risks rated **Medium** – Subject to discussions with Supervisor, Co-ordinator or Team Leader (and/or Manager), review risk treatment strategies to determine their adequacy and effectiveness. You must implement your response to risk within a few months.
- For risks rated **Low** – you should prioritise to address as and when is reasonable, ensuring that higher rated risks are prioritised.

Treatments are recorded in the Risk Register with owners and deadlines, integrated into the Corporate Plan.

13 Reporting

Reporting requirements are outlined in the Risk Management Framework, including:

- Quarterly reports to GM, Executive Committee, ARIC, and Council.
- ARIC Strategic Risk Assessment Report.
- 3 Year Risk Management Activity Plan

14 Evaluation

The effectiveness of this Procedure will be measured by performance measures out- lined in the Risk Management Framework, including risk management outcomes and compliance with procedures.

15 Document control

15.1 Review

This Procedure will be reviewed every three (3) years or as required. Minor editorial amendments may be approved by the General Manager, Director City Performance and/or Manager Governance & Risk.

15.2 Version history

The following matrix details the version history of the Risk Management Procedure.

Version	Release Date	Author	Reason for Change
1.0	14/06/2017 (Council via R&A Comm)	Coordinator Risk Management	New document
2.0	5/11/2025 (Executive Comm)	Risk Specialist	Newly adopted Procedure to align Council with legislative and regulatory changes. Title change from “Risk Management Strategy” to “Risk Management Procedure”.