

Enterprise Risk Management Framework - ERMF -

February 2022

Contents

		1
1.	0 Introduction	3
	1.1 Background	3
	1.2 Purpose	3
	1.3 Approach	4
	1.4 Office of Local Government Guidelines	4
2.	0 Principles	5
	2.1 Integration	5
3.	0 Risk Culture	7
4.	0 Roles and responsibilities for ERM	9
5.	0 Risk Assurance	11
	5.1 Three lines of defence	. 11
6.	0 Enterprise Risk Management Framework	12
	6.1 Framework design	12
	6.2 Framework elements	12
	6.3 Implementing enterprise risk management	. 13
	6.4 We perform regular risk assessments	14
	6.5 We monitor, escalate and report risks	15
	6.6 We are committed to continuous improvement	16
	Appendix 1 – Risk Management Glossary	17
	Appendix 2 – Risk Management Procedure	. 20
	Appendix 3 – Risk Appetite Statement (Confidential)	27
	Appendix 4 – Risk Matrix table	32
	Appendix 5 – Risk Owner Response	38
	Appendix 6 – Control Effectiveness Rating table	39
	Appendix 7- Risk Register Template & Instructions	
	Appendix 8 – Risk Escalation Response	46
	Appendix 9 – Risk Management Activities	47

1.0 Introduction

1.1 Background

North Sydney Council (Council) recognises that the organisation is exposed to certain risks due to the nature of its activities and the environment in which it operates. The key to Council's success is the effective management of risk to ensure its organisational objectives are achieved. Risks arise due to the organisation's operational undertakings and from external sources. Risks occur in numerous ways and have the potential to impact financial performance, reputation, health and safety, customer, community and the overall performance of the organisation.

In accordance with the Council Enterprise Risk Management Policy, Council is committed to maintaining an effective and efficient Enterprise Risk Management Framework (ERMF) to help promote a positive risk culture and proactively manage enterprise wide risks at all levels to support the achievement of Council's objectives. This is achieved through the ERMF that consists of policies and procedures that ensure risk management practices are embedded into all activities, risk management thinking is deeply entrenched into the organisation's norms and prudent risk taking is aligned to risk appetite.

1.2 Purpose

The key purpose of the ERMF is to assist Council achieve its goals and objectives in delivery programs and services as outlined in the Council Plan.

Councils' approach to ERM is designed to:

- Support the Councillors, Executive and Management to confidently make informed decisions based on organisational policy, values and appetite
- Assist Council to achieve organisational objectives through the systematic and timely identification and management of risks and strategic opportunities
- Consistently manage the effects of uncertainty through the application of robust risk management practices
- Promote compliance with relevant obligations
- Create and protect value by targeting effort and resources to the areas of highest priority.

The application of the ERMF will assist Council in:

- Protecting people, assets, finances and Council reputation
- Adopting risk treatments that are fit for purpose, cost effective and designed to reduce risk to a tolerable level
- Developing a continuous improvement culture, integrating the risk management process into overall Council processes
- Embedding a culture that promotes awareness and accountability for risk so it becomes a key part of decision making at Council.

1.3 Approach

Council acknowledges that risk is inherent in our business activities and the pursuit of our objectives. We will integrate a structured approach to the management of risk throughout the organisation in order to promote and demonstrate good corporate governance, to minimise loss and to maximise opportunities to improve service delivery and customer value. We will adopt a structured, consistent and holistic approach to the management of risk at all levels and for all business activities through the integration of business, Work Health & Safety and environmental risk management into a common framework. We are committed to incorporating risk management into critical processes and to managing risk consistent with AS ISO 31000:2018 *Risk management – Guidelines*.

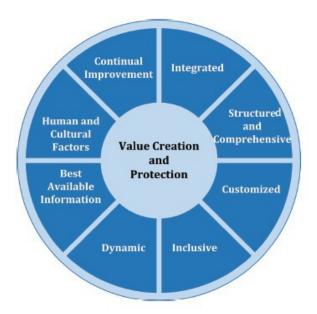
1.4 Office of Local Government Guidelines

Under the Guidelines issued by the Office of Local Government, Council is required to have a risk management framework that is consistent with the current Australian standards for risk management by 2024. This framework is compliant with this requirement.

2.0 Principles

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives. The principles outlined below provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. The principles are the foundation for managing risk:

- i) is an integral part of all organisational processes;
- ii) is systematic, structured and comprehensive;
- iii) is based on the best available information;
- iv) is tailored to the organisation's requirements;
- v) takes human and cultural factors into account;
- vi) is transparent and inclusive;
- vii) is dynamic, iterative and responsive to change;
- viii) facilitates continual improvement of the organisation.

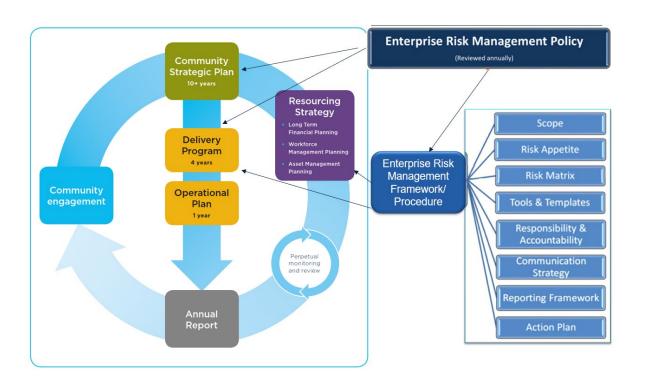


2.1 Integration

Risk management is not a stand-along activity and to be successful must be integrated into day-to-day organisational functions.

In order to maximise risk management benefits and opportunities, Council's methods and processes used to manage risk is integrated through its entire operations. It is factored into business planning, decision making, performance management, audit and assurance, business continuity and financial management.

Output from strategic and operational risk assessments is used as input to the business planning process. Council is dependent on the ERMF to be used at the strategic and departmental business level to improve performance by the organisation in the achievement of Council's strategies and actions as detailed in the Council Plan.



3.0 Risk Culture

Risk culture is a term describing the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people.

An effective risk culture is one that enables and rewards individuals and groups for behaviours and actions that are in line with policies and procedures and for taking the right risks in an informed manner. A good risk culture can be achieved in the following behaviours:

i) TONE AT THE TOP

Risk leadership¹

- We model and actively promote commitment to risk management
- We display a positive and proactive attitude toward risk and safety
- We build good relationships and a high trust environment
- We ensure compliance with policies, protocols and procedures

Responding to bad news

- We speak openly and honestly about what is working, what isn't and what still needs to change
- We identify risks, report incidents and near misses and remediate hazards without fear of blame
- We focus on identifying systemic and environmental causes, not human error

ii) GOVERNANCE

Risk governance

- We clearly define accountability for the management of risks
- We specifically address risk management in position descriptions and key performance metrics at all levels throughout organisation
- We strive to continuously improve the management of risk

Risk transparency

- We promptly share risk information across organisation
 - We share lessons learned, both positive and negative

iii) COMPETENCY

Risk resources



¹ As per ISO 31000 Standard that - 'Top Management' (e.g. GM, MANEX, etc.) are accountable for managing risk and 'Oversight Bodies' (e.g. Council, ARIC) are accountable for overseeing risk management.

- We adequately resource and support the management of risk
- We integrate risk management into our day-to-day work
- We include risk and safety every conversation and in every decision

Risk competence

- We acquire and keep up to date knowledge of risk and WHS matters
- We provide adequate information and training to ensure that we can easily identify, assess and manage risks
- We have sufficient skills and empowerment to manage risks in our area of responsibility

iv) DECISION MAKING

Risk decisions

- We communicate and understand Council's willingness to take on risks
- We seek out risk information to support informed decision-making

Rewarding appropriate risk taking

- We support those actively seeking to understand and manage risk
- We include sound risk management in Council's performance management process
- We celebrate successes and reward desired behaviours

4.0 Roles and responsibilities for ERM

The roles and responsibilities² for risk management at Council are specified in the ARIC Charter and individual position descriptions.

Personnel	Accountabilities and responsibilities
Council	 Reviews and adopts the Enterprise Risk Management Policy, endorsing the systematic approach to managing risk and opportunity across Council operations Applies risk management principles to the decision making process Reviews and considers any specific reports or recommendations that may be provided regarding the ERMF
General Manager	 Promotes a strong risk management culture by providing firm and visible support for risk management including ensuring appropriate delegations for the management of risk Ensures a Policy and ERMF is in operation to deliver a consistent approach to risk management Ensures adequate organisational structure and resourcing for risk management
Audit Risk & Improvement Committee (ARIC)	 Ensures a ERMF is in operation and delivers a consistent approach to risk management Ensures the ERMF addresses Council's exposure to both strategic and operational risks Reviews and endorses the ERMF Monitors implementation of effective risk and opportunity management controls Monitors the effectiveness of the ERMF through regular reviews and reporting Regularly reviews the strategic risk register to check that extreme and high level risks are being managed in accordance with the ERMF
Internal Audit	 Considers strategic and operational risks in the development and implementation of the Strategic Internal Audit Plan and recommending improvements Periodically audits Council's risk management practices and providing recommendations on improvement to management and the Audit and Risk Committee.
Management Executive Team (MANEX)	 Reviews and approves the ERMF Commits to, and promotes the Policy and ERMF Monitors Council's overall risk profile and mitigation strategies Ensures risk management is embedded into all critical functions and activities

² As per ISO 31000 Standard that - 'Top Management' (e.g. GM, MANEX, etc.) are accountable for managing risk and 'Oversight Bodies' (e.g. Council, ARIC) are accountable for overseeing risk management.

	 Ensures documentation of items on the risk register and ongoing and regular reviews of the risk register including the actioning of any overdue risk treatments Includes any risk treatments into business plans Empowers staff to actively be involved in managing risk Ensures Managers have the necessary knowledge and skills to effectively fulfil their risk management responsibilities and are accountable for risks arising from the activities of their departments Promotes a proactive risk culture in accordance with business management initiatives Reviews risks on the strategic risk register quarterly prior to each ARIC meeting or as otherwise may be provided as part of other reporting Reviews risks on the operational risk register at least
Executive Manager Governance	 biennially over the course of the Risk Awareness Program. Provides guidance and assistance to staff in relation to the application of the ERMF and reporting within the Strategic Risk Register Ensures relevant risk information is reported and escalated to MANEX and Audit and Risk Committee or cascaded to staff, as relevant Maintains the Risk Management Policy and ERMF to ensure its currency and accuracy and reports changes/updates in line with Council's risk management reporting cycles Manages the Strategic Risk Register and timeframes as required Provides support and advice to Managers and staff in the application and use of the ERMF as required
	Provides guidance and assistance to staff in relation to the
Executive Manager Governance	application of the ERMF and reporting within the
with Legal and Risk staff	Operational Risk Register
	Manages the Operational Risk Register and timeframes for undating and reporting as required.
	updating and reporting as required
Managers and Coordinators	 Commits to, and promotes the Policy and ERMF Ensures risk management is embedded into all critical functions and activities Ownership of risk management within business departments in accordance with this Policy and ERMF Ensures documentation of items on the relevant risk registers Ensures ongoing and regular reviews of the risk registers including the actioning of any overdue risk treatments Empowers staff to actively be involved in managing risk Promotes a proactive risk culture in accordance with business management initiatives
All staff and contractors	 Understands the risk management processes that are integrated into all Council activities Identifies, evaluates, reports and manages risks in daily activities and projects

5.0 Risk Assurance

5.1 Three lines of defence

Council operates a three lines of defence model to actively manage, monitor and oversee risk, and enhance communications on risk management and control by clarifying essential roles and duties. The model comprises the following:

1st line of defence: Departmental managers and staff

The first line of defence owns the risks attributable to their area of responsibility and are accountable for the appropriate management of risk and the effectiveness of risk controls. It is imperative that management understand and accept their accountability for owning and managing their risks. This accountability cannot be delegated to another function, such as the Risk Management team.

• 2nd line of defence: Risk management, governance

The focus of the second line of defence is to ensure that the ERMF is fully embedded and operational, and monitors the 1st line controls to ensure that risks are being effectively managed. It is a risk management function that facilitates and monitors the implementation of effective risk management practices by management, and assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout the organisation. Each of these functions has some degree of independence from the first line of defence.

• 3rd line of defence: Internal audit and External audit

The Internal Audit (IA) and External Audit functions' are independent of management and hold no operational responsibilities. IA's primary role is to provide objective and independent assurance to Council, the ARIC and MANEX, over the effectiveness and the manner in which the 1st and 2nd lines achieve risk management, control objectives and governance activities.

Assurance activity is guided by the internal audit plan. The IA plan takes into consideration Council's risk profile and targets assurance activities towards higher rated risks and/or matters of high priority to management. The internal audit plan takes into consideration the assurance activities performed by independent parties such as external audit, Audit Office of NSW, external consultants, or risk and control assessments performed by department managers.

6.0 Enterprise Risk Management Framework

A prescribed risk management framework helps establish the foundations and organisational arrangements for mandating risk management, designing the framework, implementing risk management processes, monitoring and reviewing the framework and continually improving the risk management framework.

6.1 Framework design

Council's risk management approach will follow the principles and practices specified in the Australian Standard (AS) ISO 31000: 2018 *Risk management – Guidelines* and tailored for Council's operating environment.

6.2 Framework elements

Council's enterprise risk management framework consists of a number of elements to provide a structure for a consistent risk management approach and for embedding risk management across all activities. The framework includes:

- Risk Appetite Statement: a commercial and confidential document for internal use only to help
 guide employees in respect to the parameters of acceptable risk taking and tolerances. Our
 tolerance for adverse risks will be used to determine which risks are treated through the
 development of risk treatment actions to manage risks to an acceptable level. During this
 process we will consider additional control measures to manage the risks to acceptable levels.
- Enterprise Risk Management Policy: clearly communicates Council's commitment to
 maintaining an effective and efficient risk management framework to support the
 management of enterprise-wide risks at all levels and embed risk management into day-to-day
 activities.
- Enterprise Risk Management Procedures: provides a roadmap for implementing, resourcing, communicating and improving risk management as well as measuring and reporting risk management performance. The Procedure outlines responsibilities, actions and clear step-bystep instructions for identifying, analysing, evaluating, treating and escalating risks to help Council maintain their risk register in a manner that is consistent with Council's ERMF.
- Risk Management Resources and Committees: a dedicated risk management function, Audit,
 Risk & Improvement Committee (ARIC) to provide oversight and clearly defined responsibilities
 for risk ownership and oversight.
- Training and communication: regular awareness training and communication to enhance the risk management capabilities of employees.
- Risk Management Records/System: Risk register and other risk assessment records to formally document the risk evaluation process, risk reports to communicate important risk and control information to stakeholders. Risk treatment actions and plans will be developed for risks which are unacceptable to the organisation. Risks, and the effectiveness of the risk management system will be monitored on a regular basis and we will communicate and consult with relevant stakeholders on our approach to managing risk.

 Other Supporting Policies, Procedures and Arrangements: Other supporting policies, procedures, processes, frameworks and arrangements that complement risk management including policies, procedures, internal audit, insurance arrangements, fraud and corruption plans, business continuity plans, crisis management plans, compliance plans and workplace health and safety management systems.

6.3 Implementing enterprise risk management

Council's integrated risk management approach requires an ongoing assessment of potential risks at every level. At minimum, risk management must be integrated and considered in all activities at strategic, project and operational level.

Strategic level risks

A strategy involves an informed, measurable decision about the direction an organisation chooses to take. Strategic risks arise during strategy formulation and strategy implementation or from factors in the external environment that could impact strategy.

Strategic level risks are often very hard to manage as they involve greater uncertainty, complex assumptions, complex activities and overall high inherent risk when compared to day-to-day, operational activities. The risks that are associated with strategies may be transient or relatively short term in nature but often have long lasting consequences.

Failure to manage strategic level risks could have significant negative financial, reputational and operational consequences. Therefore, a risk register is maintained for strategic level risks.

Risk and strategy are linked. Whenever there is a change to the strategy, the risks will also change. In addition, strategic plans will not remain static due to changing priorities, environmental changes, and government decisions and therefore will need re-assessment regularly.

There two distinct stages when risk need to be considered at the strategic level. When

- strategic plans are first being developed and/or refined; and
- progress is being monitored and reported on against the strategic plans.

Strategic level risks are identified and assessed by the MANEX and given formal consideration by ARIC.

If the GM cannot reduce a strategic risk to within risk appetite, the risk must be escalated to ARIC for consultation and resolution.

Operational level risks

Operational structures, systems and processes that follow strategy will give rise to operational risks. Operational level risk typically exist within the day-to-day activities and decisions at different levels across the organisation.

Operational level risks are often easier to manage than strategic level risks and project level risks as the risks are often more predictable, involve less uncertainty and can be adequately controlled through well designed and executed policies and procedures. High impact, low frequency risks can also be mitigated with appropriate crisis management, business continuity and disaster recovery planning.

A series of risk registers is maintained by risk owners at business unit level across the organisation to cover all major operational level risks. The key consideration is that risk owners need to identify and manage the risk at the most appropriate level.

All operational level risks are given formal consideration by the MANEX and ARIC.

Operational risks where the residual risk remains outside risk appetite are escalated to the MANEX and/ or ARIC with the Risk Treatment Plan(s) and monitored quarterly by the MANEX.

If the GM/ARIC cannot reduce an operational risk to within risk appetite, the risk must be escalated to Council for consultation and resolution.

Project level risks

A project is planned work or an activity that is finished over a period of time and intended to achieve a particular purpose. Projects can be related to strategic plans, major infrastructure or corporate change/ transformation activities.

Considering the inherent risks associated with projects and the level of project activity at Council, project risks need to be thoroughly considered.

All projects have risks. If the potential risks are not identified and managed early, then the project is exposed to risk of delays, safety issues, scope creep, cost over-runs and/or result in below quality outcomes.

Managing project risks is considered good management practice and an integral element of leading project management methodologies such as PMBoK.

A risk register is maintained by risk owners or by the designated Project Manager for project risks.

Project Managers are responsible for keeping their Sponsor, Steering Committee and the MANEX advised of their project/program risk profile.

Projects risks where the residual risk remains outside risk appetite are escalated to are escalated to MANEX and/ or ARIC with the Risk Treatment Plan(s) and monitored monthly by Executives.

6.4 We perform regular risk assessments

i) Risk register

The risk register is a critical element of the ERMF because it is a formal record of the risks identified, evaluated and managed by the risk owner.

A risk register is a form of risk assessment and can be maintained for a business unit, event, activity, project and strategic initiatives and cover all current and future activities, and new opportunities.

At minimum, risk registers are maintained for key risks at strategic, operational and project level.

Emerging risks should also be incorporated in the appropriate risk register as they are identified.

All risk owners are required to maintain a risk register which provides a current, accurate and complete record of risk assessment and control/management activities. The risk register is to be a "living document", remain current and subject to regular review and update as risks are addressed and new risks identified, and controls and risk treatments for current risks updated.

All risk registers are in electronic format using Council's risk register template (excel) and maintained in a shared drive to enable reporting.

The Risk Register Procedure for risk register maintenance is at **Appendix 2** and includes steps for identifying, analysing, evaluating, treating and escalating risks. This aims to help risk owners maintain their risk register in a manner that is consistent with Council's risk management framework.

The Risk Register Procedure is to be applied consistently for all strategic, operational and project risk

registers.

ii) Other risk assessments

In some instances, using Council's enterprise risk management approach, the Risk Register Procedure Instruction and the risk ratings contained in this procedure may not be suitable for some risk assessments and more context specific risks assessments are needed e.g. Onsite Safety Risk Assessment. These risk assessment activities are often identified as controls on the risk register.

Risk owners may use other more suitable risk assessment tools to manage specific and more dynamic risks, however, in all cases these risk assessments should:

- Be modelled on Australian Standard (AS) ISO 31000: 2018 *Risk management Guidelines* or the relevant standard, this Manual or best practice risk assessment methods; and
- Risk ratings and risk evaluation criteria used should always reflect Council's Risk Appetite Statement (Appendix 3).

6.5 We monitor, escalate and report risks

All employees are responsible for identifying risks and reporting those risks to their manager for consideration of the impact and level of risk.

Once a risk has been identified, managers and/or risk owners are responsible for assessing and managing the risk in accordance with Council ERMF.

Risk reporting is a shared responsibility between the risk owner and Executive Manager, Governance.

Risk reporting supports decision making for major risks identified during the risk assessment process and when balancing between risk and opportunity. Reporting arrangements can include:

- Any risk management initiatives undertaken during the period;
- Any moderate level or higher incidents or issues that have occurred during the previous quarter;
- The key inherent and residual risks facing the business unit/event/activity/project and the controls in place to manage those risks;
- Progress in implementing key risk treatment plans; and
- Any other issues that have arisen over a period or likely to arise in the future, relevant to the
 risk management framework that should be brought to the attention of the MANEX, GM and
 ARIC.

Other incidents, issues or near misses/loss events

Incidents, complaints, issues, near misses or near incidents may be leading risk indicators to an emerging risk. All employees are responsible for reporting incidents, complaints, issues, near misses or near incidents in a way consistent with the appropriate Council's policy and procedure.

6.6 We are committed to continuous improvement

Council is committed to ensuring the enterprise risk management framework and risk management activities are continually improved through learning and experience. This is achieved in a number of ways:

- Periodic review of enterprise risk management framework including Policy and Procedure;
- Communication and consultation with key stakeholders;
- Monitoring of risks, controls and treatment plans;
- Monitoring of incidents, issues and near incidents; and
- Independent review of risk management framework including an assessment of the level of risk management maturity.

Risk maturity

AS ISO 31000:2018 requires that each council continually adapts and improves the design of its risk management framework and how it is integrated throughout the council to help the council move to a higher level of risk maturity. In view of this, Council will review its risk maturity against AS ISO 31000: 2018 Standard once every three years to ensure consistent improvement in the ERM roadmap.

Version control

V	Released	Officer	Comment
1.0	21 Feb 2012	Risk manager	For Audit and Risk Committee review
1.1	08 May 2012	Risk manager	For review at Audit and Risk Committee and Management Services Committee meetings on 21 May 2012. Includes amendments as per Audit and Risk Committee comments of 21 Feb 2012
1.2	05 Jul 2012	Risk manager	For use as companion to ERM policy. Framework and context diagram in section 3 updated to reflect changes to corporate structure and business continuity planning.
1.3	21 Aug 2012	Risk manager	Updated to correspond with release of v1.1 of disruption risk mgt plans
1.4	09 Oct 2012	Risk manager	Glossary updated, particularly WHS and emergency planning terms. Standardised consequence and likelihood scales transposed from the enterprise risk assessment tool v1.9.
1.5	28 Jun 2013	Risk manager	"Framework" deleted from title. Glossary and diagrams updated
2.0	TBC	Executive Manager Governance	Document review to align to current standard and OLG draft guidelines.

Appendix 1 – Risk Management Glossary

Here are some specialist terms, and specialist uses of common terms, you will encounter in this document.

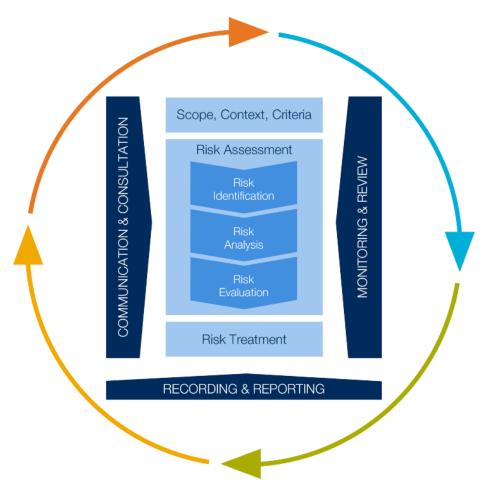
Term	Meaning
Bow tie analysis	Is a graphical depiction of pathways from the causes of an event to its consequences. It shows the controls that modify the frequency of the event and those that modify the consequences if the event occurs.
Business Objective	The primary goals of a business entity describing what the area is required to do to contribute or add value to the Council, the mission that it is charged with, business-as-usual activities, key programs and strategic business improvement initiatives.
Cause	The trigger of a risk event materialising
Consequence	Outcome of an event that impacts on the organisations objectives
Control	An activity, system or process used to reduce exposure to risk by either, preventing, detecting or mitigating risk events.
Control Design	An assessment of the adequacy of the control's design used to record how reliable the control is in mitigating the risk(s) as required.
Control Owner	The Control Owner is the individual responsible for designing, maintaining and monitoring the control.
Control Type	Identifies a control as preventative, detective or mitigating.
Enterprise Risk	A process, effected by an entity's board of directors, management and
Management (ERM)	other personnel, applied in strategy setting and across the enterprise,
	designed to identify potential events that may affect the entity, and
	manage risk to be within its risk appetite, to provide reasonable
	assurance regarding the achievement of entity objectives (COSO - Committee of Sponsoring Organizations of the Treadway Commission)
Establishing context	A step in the risk management process that involves setting the
	parameters within which risks are identified, assessed and managed.
Exception Reporting	A process established to reduce the burden of internal audit while ensuring there is a process to monitor the efficiency and effectiveness of
	the systems within the integrated risk management framework
External context	Considering the external environment in which the organisation seeks to
	achieve its objectives e.g. competitors, government policy, economic conditions.
Frequency	The estimated number of risk events in the next 12 months.
Inherent Risk	The initial risk level of an objective without the application of treatments or controls
Internal context	Considering the internal environment in which the organisation seeks to achieve its objectives e.g. internal resources, internal processes
Key Risk Indicator	Metrics that inform users about changes in the frequency or consequence of a risk.
Level of Risk	Magnitude of a risk or combination of risks, expressed in terms of the
	combination of consequences and their likelihood (SAC Rating)
	Likelihood: The chance of something happening, usually expressed in expected frequency.
	expected frequency.

Likelihood	The chance of something happening
Residual Risk	Remaining level of risk after considering existing controls or risk
	treatment
Risk	The effect of uncertainty on objectives
Risk Analysis	Process to comprehend the nature of risk and to determine the level of
	risk
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation
Risk Appetite	How much and what type of risk the organisation is generally prepared to
	accept to achieve its financial and strategic objectives.
Risk Capacity	The maximum amount of risk an entity is able to support within its
	available financial resources.
Risk Culture	A term describing the values, beliefs, knowledge, attitudes and
	understanding about risk shared by a group of people.
Risk Tolerance	The maximum amount or type of risk the entity is prepared to tolerate
2: 1 2 6:	above risk appetite
Risk Profile	Risk profile is the amount or type of risk the organisation is currently exposed to. Forward risk Profile is forward looking view of how the
	organisation's risk profile may change under both expected and stressed
	conditions, i.e. financial.
Risk Acceptance	The assumption of a risk, typically because its risk reward profile is
Tilsk / teeeptanee	attractive and within your risk tolerance. In general, it is impossible to
	make gains in business or life without taking risks. As such, risk
	acceptance is a common risk treatment.
Risk Evaluation	Process of comparing the results of risk analysis with risk criteria to
	determine whether the risk and/or its magnitude is acceptable or
	tolerable
Risk Identification	Process of recognising and describing risks
Risk Management	Coordinated activities to direct and control an organisation with regard
	to risk.
Risk Management	Set of components that provide the foundations and organisational
Framework	arrangements for designing, implementing, monitoring, reviewing and
2112	continually improving risk management throughout the organisation
Risk Management Process	Systematic application of management policies, procedures and practices
	to the activities of communication, consulting, establishing the context,
	and identifying, analysing, evaluating, treating, monitoring and reviewing risk
Risk Matrix	A tool for ranking and displaying risks by identifying ranges for
NISK WIGHTA	consequence/impact and frequency.
Risk Owner	Person or entity with the accountability and authority to manage a risk.
Risk Priority	Rating established through the assessment of likelihood and
,	consequences that provides a priority for action, also known as the risk
	rating or severity assessment code.
Risk Register	A formal record or repository (system or file) of the risks identified,
	evaluated and managed by the risk owner.
Risk Tolerance	The level of variation from the pre-determined risk appetite an
	organisation is prepared to accept
Risk Treatment	Selection and implementation of an action or process identified to
	address or mitigate a risk.
Root Cause Analysis	A systematic approach to investigating incidents or complaints that
	includes the identification of the contributing factors within the systems.

Severity Assessment Code	A process for assessing the consequence and frequency that includes descriptors to create a consistent approach of applying a rating
Severity - Financial	The "estimated typical loss per event", i.e. a single event and is assessed on a gross loss basis (i.e. insurance is not considered)
Severity Non-Financial	The estimated non-financial (reputational, regulatory, staff health and safety, business disruption and management effort) impact per event.
Stakeholder	A person or organisation that may affect, be affected by, or perceive themselves to be affected by, a decision or activity.
Strategic Risk	A source of uncertainty that may arise in pursuit of strategic objectives. The risks and uncertainties associated with carrying out of the strategic objectives as articulated in high level plans; strategic programs/initiatives. Strategic risks arise during strategy formulation and implementation or factors from the external environment that could impact strategy.

Appendix 2 – Risk Management Procedure

This Risk Management Procedure reflects the Australian Standard (AS) ISO 31000: 2018 Risk Management – Guidelines. The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk. This process is illustrated below.



Following this Procedure will help risk owners manage their risks and maintain their risk register in a manner that is consistent with Council's enterprise risk management framework.

This Risk Management Procedure should be read in conjunction with:

- Appendix 3 Risk Appetite Statement (Confidential)
- Appendix 4 Consequences Rating Table
- Appendix 5 Risk Owner Response Table
- Appendix 6 Control Effectiveness Rating Table
- Appendix 7 Risk Register Template & Instructions
- Appendix 8 Issue Escalation Response

Communication and consultation

The purpose of communication and consultation is to assist relevant stakeholders and employees in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Communication seeks to promote awareness and understanding of risk.

Effective communication and consultation with key stakeholders regarding risk management processes, issues and initiatives is critical to the success of Council's risk management framework. Employees must ensure that relevant stakeholders are informed, consulted and, if necessary, involved in risk management activities that affect them or for which they may be able to contribute. In particular, stakeholders who may be effected by, or may have knowledge regarding, risks must be consulted regarding the assessment and evaluation of such risks

Scope, context and criteria

Establishing the scope, context and criteria helps to customize the risk management process, enabling effective risk assessment and appropriate risk treatment.

The scope of risk management activities are enterprise wide. The risk management is applied at different levels (e.g. strategic, operational, programme, project, or other activities).

Context of the risk management process should be established by understanding of the external and internal environment in which Council operates and should reflect the specific environment of the activity to which the risk management process is to be applied. Important considerations when determining context include:

- What do we want to do or achieve? Define the desired outcomes of the event, activity or project.
- How will we know we have been successful? Identify the success measure or measures for each desired outcome. For established activities, success measures should have been developed and agreed during the development of Council's hierarchy of plans.
- Council's external environment social factors, demographics, economic, environmental.
- Council's stakeholders MANEX, residents, customers, regulators, employers, councillors, mayor, media, insurers, service providers, staff and casual employees.
- Council's internal environment goals, objectives, culture, risk appetite/tolerance, organisational structures, systems, processes, resources, key performance indicators and other drivers.
- Council's appetite for risk this is the amount of risk that Council is willing to accept in pursuit of its
 objectives.

Risk criteria should be established at the beginning of the risk assessment process. It specifies the amount and type of risk that Council may or may not take, relative to objectives. The risk appetite statement, risk matrix table and control effectiveness tables will help establish criteria for assessing, managing and taking risk.

Risk assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. Risk assessments (including risk registers) should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiry as necessary.

The first step to conducting the risk assessment is to ask risk owners to validate the business objectives of that business area. Where possible, the business objectives of that business area should also be sourced, i.e. what the area does to contribute or add value to the Function Unit/Department/Project, or the mission that it is charged with. These are likely to be identified through the business planning process.

In addition to the business-as-usual objectives, key programs and strategic improvement initiatives should also be identified. The number of objectives will depend on the size of the business area. However, on average, 4-10 key objectives should be identified.

Risk identification

Risk identification is the process of identifying risks facing Council. This involves thinking through the sources of risks, the potential hazards and opportunities, the possible causes and the potential exposure.

The aim of this step is to generate a comprehensive list of key risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. 'Key' risks are managements' view of the most serious threats to the business objectives.

Risk identification occurs within the context of the risk management activity, procedure or process. The following categories of risk should typically be considered:

- Business activities/Strategic/External threat risks;
- Legal / Liability risks;
- Financial risks;
- Reputational risks;
- IT/Security/Cyber/ Business disruption risks;
- Community /Public health & safety risks;
- WHS & staff wellbeing risks;
- Environmental risks; and
- Asset and Infrastructure risks

It is important to undertake a systematic and comprehensive identification of all risks including those not directly under the control of Council because a risk that is not identified at this stage will not be included in further analysis. The key questions when identifying risks are:

- What can happen?
- Where can it happen?

- When can it happen?
- Why can it happen?
- How can it happen?
- What is the impact?
- Who is responsible for managing the risk?

Council may utilise a number of methods to help identify risks that could materially impact the business. These include:

- Brainstorming
- Formal risk workshops and consultation with stakeholders
- Bow-tie analysis
- Periodic working/project committee meetings
- Periodic reviews of the risk register
- Scenario analysis
- Business process reviews and work breakdowns
- Review of actual incidents and issues identified
- SWOT analysis

It is also important to consider the potential causes of a risk as it will help to address the risk - the next stage of the risk management process. Some causes of risk could include:

- commercial/legal relationships
- socio-economic factors
- political/legal influences
- personnel/human behaviour
- financial/market activities
- management activities and controls
- technology/technical issues
- the activity itself/operational issues
- business interruption
- natural events

Risk Analysis & Evaluation

Once risks have been identified, they are then analysed. Risk analysis involves consideration of the causes and sources of risk, their positive and negative severity, their key controls and the frequency that those consequences can occur. The following risk criteria should be used as a guide when analysing risks.

Control identification & assessment

Once you have determined the potential risk events, you need to identify and consider the current controls (people, systems and processes) you have in place to mitigate the risk. To then understand the extent to which the likelihood and consequence of a risk occurring is being mitigated, the full suite of controls in place must be documented and assessed for effectiveness of design and operation. The assessment should only assess controls that are currently in operation, not those that are planned.

A control can include a policy, procedure, plan, manual, devise or action that reduces a risk from occurring. A control can reduce the likelihood and/or the consequence of a risk. Each control should also be assigned a Control Owner. The Control Owner is the individual responsible for designing, maintaining and monitoring the control. The Control Owner may be from another business area.

The control type should also be identified. Control type can be:

- Preventative: Controls in place to prevent or stop a risk event from occurring e.g. system security, training etc.,
- Detective: Controls in place to identify that an event has occurred e.g. exception report, or
- Mitigating: Control that reduce the impact of risk events that have occurred e.g. insurance.

Once you have identified these current controls, you need to assess the control's design and performance to determine the overall control effectiveness. To determine control effectiveness, think about the quality of documented policies and procedures, adequacy of training, staff turnover, and recent issues - see **Appendix 6** for a guide on control effectiveness assessment.

Residual risk assessment

Likelihood/ Frequency is defined as the probability that the risk event will occur within the next 12 months.

The consequence/severity assessment is the effect or impact of the risk event. We will utilise the consequences ratings shown in Appendix 4.

A four-level rating scale applies to each of these factors, as illustrated in the table below. The greatest of the four dimensions should be used to determine the overall consequences, i.e. if reputation damage, regulatory and staff health and safety impacts were estimated as Low, but business disruption and management effort is assessed as Medium; the overall impact should be assessed as Medium.

Risk Response

Once the risk assessments are complete, the Risk Owner must determine the appropriate response to the risk. We uses four response categories, as detailed in the **Appendix 5**. When determining the risk response, the risk assessment and risk appetite should be considered, i.e. if not within appetite, the response should be 'active management'.

Residual risk is the exposure to a risk having considered the overall control effectiveness (Appendix 6). During risk evaluation, if the risk response for any of the identified risks is 'Consider control improvement', or 'Active management', an issue or action may be required. Where this is the case, the issue/action

should be identified by the Risk Owner within or post-workshop. The issue/action should then be managed in accordance with the Issues Escalation Guidelines in **Appendix 8**.

The actions and level of control and/or risk treatment will depend on the risk level.

High or Extreme Risk: Requires immediate risk treatment as the potential risk exposure could be devastating to the organisation.

Medium Risk: May require action at some point in the near future, as it has the potential to be damaging to the organisation

Low Risk: Low risks are generally acceptable and do not require any formal sign off. Low risks should continue to be monitored and re-evaluated on a regular basis. Low risks can generally be treated with routine procedures.

Risk Treatment / Action Plan

If the risk response for any of the identified risks is 'Consider control improvement', or 'Active management', an issue or action may be required. Where this is the case, the issue/action should be identified by the Risk Owner within or post-workshop. The issue/action should then be managed in accordance with the Issues Escalation Guidelines in Appendix 8.

Risk treatment involves selecting one or more options for modifying risks and implementing those options. Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include the following:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing the risk in order to pursue an opportunity;
- removing the risk source;
- changing the frequency/likelihood;
- changing the impact/severity;
- sharing the risk with another party or parties (including contracts and risk financing); and
- retaining the risk by informed decision

The information provided in risk treatment plans should include:

- the reasons for selection of treatment options, including expected benefits to be gained;
- those who are accountable for approving the plan and those responsible for implementing the plan;
- proposed actions;
- timing and schedule.

Monitoring and Review

Few risks remain static. Risks will be continuously monitored and reviewed; and the effectiveness of the controls in place and of the risk treatment/action plans will be assessed to ensure changing circumstances do not alter risk priorities.

The results of monitoring and review are incorporated within Council's performance management, measurement and reporting activities.

Risks will be monitored regularly in line with their significance. At minimum, the risk register will be reviewed quarterly as part of the operational plan review process.

Feedback on the implementation and the effectiveness of the ERM Policy and ERMF will be obtained from the risk reporting process, internal audits and other available information.

Recording and reporting

The risk management process and its outcomes will be documented and reported through appropriate mechanisms. Risk management records include:

- Risk registers maintained by Council for strategic risks, operational risks and other types of risks
- Other forms and types of risk assessments conducted for the purpose of identifying, evaluating and managing risk

Records should be maintained within Council's formal record management system.

Periodic risk management reporting and / or risk dashboards aims to enhance the quality of dialogue with the MANEX, ARIC, stakeholders and oversight bodies. Risk reports communicate important risk and control information.

Appendix 3 – Risk Appetite Statement (Confidential)

Risk Category	Sub-risk categories/components	Risk Appetite	RAS Statement	Risk Tolerance (Council will not tolerate - AVOID):	Council can tolerate (ACCEPT)
Finance	Budget allocation (including recurrent), accounts payable, contingent liability, fixed assets, capital programs, inventory, payroll, procurement, trust accounts.	Medium	Council recognises the financial risks involved in delivering a wide range of services, programs and capital projects. Council will seek commercial opportunities but always maintain a prudent financial management approach.	Council will not tolerate: - Risk which may have a significant negative impact on Council's long term financial sustainability or are highly speculative - Maladministration, misuse, serious or substantial waste of project funds or resources. - Negligent or uninformed decisions that have a significant negative impact on Council's financial sustainability. - Material mis-statement in financial accounts. - Serious or persistent breach of financial policies and delegations.	Council can tolerate: - Calculated financial risks to deliver important infrastructure, improve service delivery or promote ecological sustainability - Minor unforeseen/ unavoidable cost variations of business unit budget to meet community needs or pursue commercial or innovation opportunities Projects delivered within provided contingency and with required reporting within the adopted and endorsed reporting structure.
WHS/ Safety	HR Management, Education / Training, Equity and Diversity, Industrial Relations, HR Management, Education and Training Equity and Diversity, Industrial Relations, Conflict Resolution, Leave Management, Work Health and Safety, Organisational Wellbeing, Recruitment, Retention, Transfer and Promotion, Performance management, discipline, delegations, relationships/teams, Fire	Low	Council has no appetite for work practices, actions or inactions that compromise the wellbeing and safety of people - including staff, contractors and community. Council will pursue a healthy and engaged workforce based on respect.	Council will not tolerate: - Avoidable lost time injuries or illness or risks that have a long term impact on staff health, wellbeing or morale Practices that knowingly compromise workplace or worker safety Activities that result in reasonably foreseeable and preventable fatalities, harm, serious injuries or illnesses to workers Increases in near miss events which is not subsequently mitigated or managed.	Council can tolerate: - Minor incidents or injuries that occur in undertaking normal business activities despite best efforts to avoid or mitigate - Minor unforeseen incidents or injuries that that arise from time to time in the course of undertaking normal activities Moderate impact issues relating to improving workforce planning.

Risk Category	Sub-risk categories/components	Risk Appetite	RAS Statement	Risk Tolerance (Council will not tolerate - AVOID):	Council can tolerate (ACCEPT)
	prevention, fire suppression, Fire Investigation, Community capacity, wildfire management, employee well being;				
Environmental	Pollution, Carbon Trading, Land Management, and water availability, Impact of Operations on the Environment, Climate change, Energy efficiencies and carbon, Greenhouse gas emissions, Deforestation, Waste management, Air /light/ noise pollution, Biodiversity and habitat, Contaminated land, Material sourcing and resource efficiency, hazardous substances	Low	Council is prepared to make decisions that promote ecologically sustainable development. In making decisions and whilst undertaking various activities, Council has a low appetite for natural environmental damage arising from normal business activities (subject to financial sustainability).	Council will not tolerate: - Risk which may have significant long term negative environmental consequences, sustainability or that are highly speculative - Activities and practices that knowingly compromise the environment, are reasonably foreseeable and preventable.	Council can tolerate: - Calculated minor and /or short term environmental impacts where it is necessary in order to achieve key objectives - Minor environmental impacts (e.g. biological diversity and ecological integrity) from uncontrollable or unforeseen events.

Risk Category	Sub-risk categories/components	Risk Appetite	RAS Statement	Risk Tolerance (Council will not tolerate - AVOID):	Council can tolerate (ACCEPT)
Reputation	Professionalism, Customer Satisfaction, Perceptions of Safety, Public Complaints, Fraud Corruption/Criminality, Internal Investigations, Public Interest Disclosure; Community; Media profile;	Low	Council recognise the importance of protecting its reputation. Council understands that negative publicity may occur as a consequence of making decisions in an environment where there are competing stakeholder priorities and interests and is prepared to take on some level of risk for actions that may result in reputational damage where Council can justify and explain the reasons for its decisions.	Council will not tolerate: - Long term sustained negative publicity that damages Council's reputation and takes a long time to repair - Inadequate consultation with key stakeholder's that results in a major disruption and formal crisis management Situations where key stakeholders lose confidence in Council's capabilities.	Council can tolerate: - Localised, short term negative publicity as a consequence of making decisions in an environment where there are competing priorities and interests - Very low level complaints associated with changes in policy from a changing political environment but with a quick response to managing community complaints - Isolated minor incidents, concerns and complaints that can be resolved by day-to-day management - Where a reputational risk can be explained.
Legal /Liability	Regulatory Control over service, Internal and External Audit, legislation, regulatory compliance, Fraud Corruption, COI, planning for local laws, building etc Governance (Privacy, FOI, CoC, authority of council, structure)	Low	Council has little or no appetite for significant breaches of legal obligations or contractual arrangements that result in fines, penalties or significant reputational damage. Council is committed to achieving compliance in all areas of its operations.	Council will not tolerate: - Risks which may give rise to extensive litigation/ indictable offences - Any fraudulent, unethical and corrupt conduct Any instances where Council Officials knowingly break the law, fail to comply with legal obligations or knowingly breach internal policies Risks that cause inaccurate reporting or breaches of statutory deadlines	Council can tolerate: - Calculated risks which may give rise to isolated complaints that are incidental to normal business activities despite best efforts to avoid or mitigate - Minor impact breaches that are unforeseen - Short-term noncompliance due to unrealistic regulatory timeframes after completion of risk assessment.

Risk Category	Sub-risk categories/components	Risk Appetite	RAS Statement	Risk Tolerance (Council will not tolerate - AVOID):	Council can tolerate (ACCEPT)
Business activities (assets & infrastructure)	Business continuity, contract management including (tendering), outsourcing, project management, intellectual property, sponsorship, customer service delivery, internal controls, technical. Physical assets, security of assets and infrastructure. Condition of infrastructure.	Medium	Council is willing to transform and embed changes in many parts of business activities through the lesson learnt, resilience developed and innovations pivoted to support quality of life and values in the community.	Council will not tolerate: - Risks from a lack of due diligence in Statutory planning and legislative approval on assets - Risks that disrupt any Council critical services beyond three days and other less critical services as per Council's established maximum tolerable outages in the Business Continuity Plan Significant or ongoing loss of corporate knowledge that results in service interruptions and impacts key stakeholders Loss of asset and infrastructure and functionality in the future and due before its lifecycle.	Council can tolerate: - Minor disruptions to critical Council services or short term disruption to less critical services within council's Business Impact Analysis - A level of business interruption in the short term where it will ultimately benefit service delivery in the long term - Business activities interruptions where there is a balance with potential for innovation improvements - Moderate impacts to service delivery issues due to new technology or innovation initiatives.
Community / Public health & Safety	safety, emergency events, diversity, health wellbeing, skills and opporunities, active living; pandemic planning and response;	Medium	Council is focussed on enhancing liveability, safe and connected communities through supporting people to enjoy safe and active lives and public safety.	Council will not tolerate: - Risk that may severely disrupt ability to conduct core daily activities/ services - Risks that severely impact public property or safety - Risks that severely impact public health - Risks that impact public safety due to poor practices by contractors - Risks that leave public asset/infrastructure in an unsafe situation in a certain period of time within the safety standard - Risks that result in non-compliance with public amenities and safety measure - Risks that significantly negatively impact North Sydney's social wellbeing and quality of life for our community.	Council can tolerate: - Risks that result in some inconvenience to the community that is necessary in order to achieve key objectives and public safety Calculated risks/threats that diminishes our efforts to build and maintain strong relationships with agencies, to manage emergency events and community Calculated risks /threats that support and prioritise community service, safety and delivery during triage situation moderate impacts on North Sydney's social well being and quality of life due to new approaches or innovative initiatives.

Risk Category	Sub-risk categories/components	Risk Appetite	RAS Statement	Risk Tolerance (Council will not tolerate - AVOID):	Council can tolerate (ACCEPT)
Information Management and Technology	Cyber, data privacy, information risks	Low	Council's aim is to protect our assets held in our information technology systems. Council may be prepared in some circumstances to take a moderate level of risk in order to deliver more innovative services efficiently and effectively; connected to community through digital media.	Council will not tolerate: - Risks which may give rise to extensive and total loss of functions across the organisation - Failure to escalate essential service outages to CEO within 2 hours. - Loss of corporate knowledge that results in service interruptions and impacts key stakeholders. - Intended data leakage or breaches of privacy - Risks which may give rise to extensive and total loss of functions across the organisation -Loss of corporate data and information that results in service interruptions and impacts key stakeholders. - Risks which threatenCouncil IMT security and privacy on customer data - Failure to respond to IT incidents and events	Council can tolerate: - Calculated risks relating to minor downtime or scheduled outage in a single area that are incidental to normal business activities despite best efforts to avoid or mitigate - Unforeseen interruptions from uncontrollable events of up to the maximum allowable for any system (IM&T business continuity planning). - Minor reputational impact from one-off community complaints relating to service quality. - Moderate impacts to service delivery issues due to new technology or innovation initiatives or new improvements.

Appendix 4 – Risk Matrix table

Frequency/Likelihood:

Likelihood:	Definition – the extent to which an event is likely to occur Likelihood is measured as the probability that the risk event will occur within the next 12 months.				
	Rating Probability		Frequency / Commentary		
А	Almost Certain	> 75%	The situation or event is expected to occur in most circumstances. May occur within 12 months		
В	Likely	50 to 74%	The situation or event will probably occur in most circumstances. May occur within 1-2 years		
С	Possible	25% to 49%	This situation or event might occur at some time. May occur 3-5 years		
E	Rare	The situation or event may occur in exceptional circumstances.	Not likely to occur within the next 5 years.		
	Considerations include: ② actual history (of similar internal and external events) incl. observed volatility ② economic conditions ② frequency of risk events or volume of transactions ③ number of / complexity of related processes				

Overall risk levels

CONSEQUENCE LEVEL Critical Medium High Low Almost 10 11 15 16 certain LIKELIHOOD LEVEL Likely 9 14 13 7 8 12 Possible 3 1 2 5 6 Rare

Risk Levels				
12-16 Extreme				
5-11	Moderate			
1-4 Low				

Severity / Consequences – Financial and Non-Financial Impact

Risk Categories	Sub-risk categories/components	Critical	High	Medium	Low
Finance	Budget allocation (including recurrent), accounts payable, contingent liability, fixed assets, capital programs, inventory, payroll, procurement, trust accounts.	> \$3m Loss of assets, adverse impact on corporate budget. > 30% Loss of assets, adverse impact on business unit budget. External audit qualification. Requires State or Federal intervention.	'->\$1m to \$3m Loss of assets, adverse impact on corporate budget - 15% to 30% Loss of assets adverse impact on business unit budget Internal Auditor or General Manager review qualification Major, longer negative implications for Council's ability to finance delivery of capital projects and/or services.	- \$300k-\$1m Loss of assets, adverse impact on corporate budget 5% to 15% Loss of assets, adverse impact on business unit budget Internal review from Business Unit Manager	- < \$300k Loss of assets, adverse impact on corporate budget; - < 5% of Loss of assets, adverse impact on business unit budget
Reputation	Professionalism, Customer Satisfaction, Perceptions of Safety, Public Complaints, Fraud Corruption/Criminality, Internal Investigations, Public Interest Disclosure; Community; Media/communication profile; Political;	- Significant number of community complaints and/or extended adverse national media coverage - Reputation impacted with large majority of key stakeholders Significant and irreparable breakdown of strategic and/or business partnerships Ministerial intervention, appointment of Commissioners, or Regulator involved in issue resolution etc Critical loss of credibility	- A noticeable increase in the volume of community complaints and/or short-term adverse national media coverage - Reputation impacted with a significant number of stakeholders; - Criticism by other agencies or scrutiny by external authority such as the Local Government Inspectorate, Auditor General etc Breakdown of strategic and/or business partnerships taking considerable effort to repair relationships Serious loss of credibility	- Complaints from a small number of community and/or limited adverse local / state media coverage - Reputation impacted with some stakeholders Criticism by other agencies or scrutiny by internal committee or internal audit to prevent escalation Some loss of credibility requiring effort to regain	- Complaints from a relatively small number of community with no media coverage - Issue resolved promptly by day to day management processes Little or no stakeholder interest. Internal review only Temporary image degraded within department

Risk Categories	Sub-risk categories/components	Critical	High	Medium	Low
			requiring major effort to regain		
WHS / Safety	HR Management, Education / Training, Equity and Diversity, Industrial Relations, HR Management, Education and Training Equity and Diversity, Industrial Relations, Conflict Resolution, Leave Management, Work Health and Safety, Organisational Wellbeing, Recruitment, Retention, Transfer and Promotion, Performance management, discipline, delegations, relationships/teams, Fire prevention, fire suppression, Fire Investigation, Community capacity, wildfire management, employee well being;	- Serious injury resulting in hospitalisation and/or significant compensation or public liability claim; Notification to and investigation by SafeWork NSW - Potential / actual death of staff member(s) or Long term duration lost time injury of >10 days Potential for wide-spread impact on staff health or safety; Severe loss of critical skills, key people and business knowledge, programs/strategies are not delivered. - Widespread poor engagement and staff moral with high staff turnover. Inability to attract talented staff to numerous roles	- Major injury to staff as a result of an WH&S issue or potential for short-term wide-spread impact on staff; Medium duration lost time injury of 7-10 days. - Loss of critical skills and key people, programs/strategies cannot be delivered; - Capacity to attract quality staff is significantly compromised - Major industrial disputes - Potential for short-term wide-spread impact on staff	- Minor breach of legislation (WHS/employment laws) People require minor medical treatment Short duration lost time injury of 3-7 days Some short term localised impact on staff morale, community or customer relations Minor injuries or illness from normal activities treated by first aid.	- Loss of a staff member from work through injury or illness treated by first aid Localised concerns by staff, community or customers Minor incident or 'near miss' No lost time.

Risk Categories	Sub-risk categories/components	Critical	High	Medium	Low
Legal/liability	Regulatory Control over service, Internal and External Audit, legislation, regulatory compliance, Fraud Corruption, COI, planning for local laws, building etc Governance (Privacy, FOI, CoC, authority of council, structure); EPAs;	'- Significant breach leading to investigation by external agency resulting in successful prosecution or sacking of Senior Officers, '- Council/ elected representatives, administrator appointed Practice standards breach personal privacy and human rights across the organisation - Severe sanction from regulator resulting in successful prosecution or sacking of Senior Officers;	- Major breach or systemic breaches leading to investigation by external agency e.g. ICAC resulting in negative findings, fines or penalties or orders or loss of licence or loss of service; - Adverse directive issued by regulator to senior management or board; - Breach of regulation with investigation or report to authority with prosecution and/or moderate fine possible	- Technical breach of legislation resulting in small fine, warnings, investigation finding technical breach of legislation and improvement notices issued A high threat of legal action. Crisis management required. - Escalation in supervision by regulator resulting in increased reporting requirements; Minor legal issues, non-compliances and breaches or regulations.	- Minor breach of legislation, isolated complaint or incident where there is a threat of legal action that can be resolved by management.
Environmental	Pollution, Carbon Trading, Land Management, and water availability, Impact of Operations on the Environment, Climate change, Energy efficiencies and carbon, Greenhouse gas emissions, Deforestation, Waste management, Air /light/ noise pollution, Biodiversity and habitat, Contaminated land, Material sourcing and resource efficiency, hazardous substances	- Severe widespread damage or irreversible impact on environment - Detrimental long term environmental impact Total destruction of a species, habitat or ecosystem Requires over 10 years repair National media interest Notification to authority required. Civil prosecution Event results in commencement of prosecution of Council or Council staff by Environment Protection Authority	- Large but local impact on environment Long term but reversible impact on environment taking greater than 5 years to recover and requiring significant restorative work Environmental damage is evident Local media interest Repeat community complaints Regulatory enforcement action (e.g. fine, notice, order) Event results in issuance of significant fine to Council or Council staff by	- Medium term impact on environment requiring moderate restorative work Environmental impact is evident Up to 2 years recovery period Does not impair the overall condition of the habitat or ecosystem Event results in issuance of on the spot fine to Council or Council staff by Environment Protection Authority	- Minor short term impact on environment such as remote temporary pollution that can be remedied quickly Brief, non-hazardous pollution or damage or negligible environmental impact No discernible impact or measurable impairment Minor clean up required No impact on the overall condition of the habitat and ecosystem Event results in notification to Council or Council staff by Environment Protection Authority

Risk Categories	Sub-risk categories/components	Critical	High	Medium	Low
			Environment Protection Authority		
Business activities (assets & infrastructure)	Business continuity, contract management including (tendering), outsourcing, project management, intellectual property, sponsorship, customer service delivery, internal controls, technical. Physical assets, security of assets and infrastructure. Condition of infrastructure.	- Inability to deliver critical programs, projects and/or services for >7 days. > 4 weeks project time slipage Significant adverse impact on servicess visibly obvious to key stakeholders Major scope changes and noticeable quality degregation require redesign Complete destruction/collapse and denial of access to asset or infrastructure	- Severe and widespread decline in services. Relationship with stakeholders/ key suppliers becomes strained Inability to deliver critical programs and/or services for 4-7 days 3-4 weeks project time slipage Noticeable quality degregation require remediation and Council approval, possible safety issues Partial destruction/collapse and denial of access to asset or infrastructure - Major loss of business with long term significance	- Some delays in meeting stakeholder requirements < 1 week project time slipage Noticeable decline in service levels - Unscheduled short term disruption for up to 1 business day Failure of infrastructure and asset creates slight inconvenience to users - Moderate loss of business with long term significance	- Scheduled interruptions An inconvenience with minimal or no adverse impact on projects or other service activities Unscheduled interruptions for less than 4 hours Little or no impact on delivery program Infrastructure or asset is subject fails causing minor delays and is subject to routine maintenance

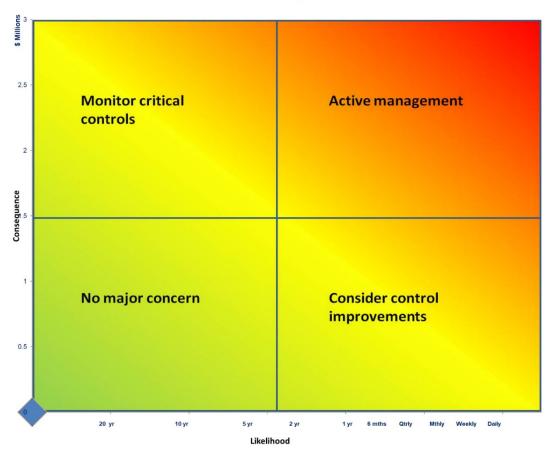
Risk Categories	Sub-risk categories/components	Critical	High	Medium	Low
Community / Public health & Safety	safety, emergency events, diversity, health wellbeing, skills and opportunities, active living; pandemic planning and response;	- Extensive disruption to facility or services > 12 months - Any fatalities or extensive long term injuries; worst case loss to organisation - Civil commotion and riot; - Serious or life threatening injury or multiple serious injuries causing hospitalisation.	 Public protests and dislocation. Potential for significant psychological or physical harm to sectors of the community. Significant injury involving medical treatment or hospitalisation; high loss to organisation Major disruption to facility or services up to 3 months Damage to relationships and loss of support; 	- Considerable disruption or inconvenience to sectors of the community up to 2 weeks; - Medical treatment Injury	- Some inconvenience to the community or minor disruption to facility or services less than a week; primarily acceptance and approval exists; - Injuries or ailment not requiring medical treatmen
Information Management and Technology	Cyber attack, data privacy, information risks, loss of data	- IT Services not available wide for > 2 days or more - Total and persistent and lengthy loss of IT capacity for several areas of Council or whole of Council - Significant loss of data resulting disclose of data exposure to public; - Power outage for more than 2 days;	- IT Services not available for > 1 day Notable, persistent and lengthy IT disruption / deterioration of systems perfomance for multiple/all service areas OR sustained disruption of many significant applications	- IT Services not available for up to 5 hours - Some IT disruption / deterioration of systems perfomance for one or two service areas OR some disruption of a significant application	- Short infrequent disruptions to IT Services (<1-2 hours during office hours) or low IT disruption / deterioration of systems perfomance - Low downtime or outage in single area of organisation

Appendix 5 – Risk Owner Response

Risk response	Guidance
No major concern	Risk has low severity/impact and frequency – review for possible redundant controls. Otherwise, no further action is required.
Monitor critical controls	Monitor critical controls so that they appropriately respond to rare but high-severity/impact events.
Consider control improvements	Consider control or process improvement opportunities to improve overall performance.
Active management	Actively manage these high-impact, high-frequency risks through close supervision and appropriate control assurance programs. Take action, where appropriate, to reduce, avoid or transfer the risk. Remediate ineffective controls or improve the control environment to reduce risk.

Heat Map

Risk Owner Response Matrix



Appendix 6 – Control Effectiveness Rating table

Control design

Evaluation	Guidance
Adequate	Control design is reliable in mitigating the risk(s) as required.
Substantially Adequate	Control design is reliable in most cases; however, marginal improvement is needed to mitigate the risk(s) as required.
Inadequate	Design of the control is unreliable; control design requires substantial improvement to mitigate the risk(s) as required.

Control performance /Operating Effectiveness

Evaluation	Guidance				
Effective	Control performance is reliable in mitigating the risk(s) as required.				
Substantially Effective	Control performance is reliable in most cases; however, marginal improvement is needed to mitigate the risk (s) as required.				
Ineffective	Performance of the control is unreliable; control performance requires substantial improvement to mitigate the risk(s) as required.				

Overall control effectiveness

Evaluation	Guidance
Effective	Overall, the design and performance of related controls are reliable in mitigating the risk as required.
Substantially Effective	Overall, the design and performance of related controls are reliable in most cases; however marginal improvement is needed to mitigate the risk as required.
Partially effective	Overall, the design and performance of related controls are reliable only in limited circumstances and require a marked improvement to mitigate the risk as required.
Ineffective	Overall, the design and performance of related controls are unreliable in mitigating the risk as required.

	Inadequate	Ineffective	Ineffective	Ineffective
Design	Substantially adequate	Substantially effective	Partially effective	Ineffective
	Adequate	Effective	Substantially effective	Partially effective
		Effective	Substantially effective	Ineffective

Performance

Appendix 7- Risk Register Template & Instructions

	STEP 1: RISK IDENTIFICATION & ANALYSIS STEP 2: RISK EVALUATION							STEP 3: RISK TREATMENT										
STEP 1: RISK IDENTIFICATION & ANALYSIS				RISK MITIGATION /UPSIDE RISKS				RISI	(ASSESSMENT	- RESIDUA		DEVELOP RISK TREATMENT PLAN		STEP 4:				
#		Sources of risk/ Causes; Impact	Strategic Goal Impacted	MANEX Risk Owner	Risk Category	Risk Appetit e	Current Controls	Control Design	Control Operating	Overall Control Effectiveness		Consequence	Rating	Within Risk Appeti	Action	Owner	Due Date	ESCALATE
1					Finance	Medium		Adequate	Effective	Effective	4 Almost	1 Low	4 Low	Yes -				
2					Environmen tal	Low		Adequate	Ineffective	Partially effective	4 Almost	4 Critical	16 Extreme	No -				
3					Reputation	Low		Adequate	Effective	Effective	3 Likely	2 Medium	6 Moderate	No - Escalate				
4					Legal /Liability	Low		Adequate	Substantially	Substantially	1 Rare	1 Low	1 Low	Yes -				
5					Business	Medium		Adequate	Ineffective	Partially	3 Likely	2 Medium	6 Moderate					
6						Medium		Adequate	Effective	Effective	3 Likely	2 Medium	6 Moderate					
7					Information	Low		Adequate	Substantially	Substantially effective	2 Possible	2 Medium	4 Low	No -				
8					WHS / Safety	Low		Inadequate	Ineffective	Ineffective	3 Likely	2 Medium	6 Moderate					
9					WHS / Safety	Low		Substantiall v adequate	Effective	Substantially effective	3 Likely	2 Medium	6 Moderate					

The purpose of this Risk Register Template & Instructions is to provide step-by-step instructions for completing the risk register to help risk owners maintain their risk register in a manner that is consistent with Council's Enterprise Risk Management Framework. To complete the risk register, you will need:

- Appendix 3 Risk Appetite Statement (Confidential)
- Appendix 4 Risk Matrix Table
- Appendix 5 Risk Owner Response Table
- Appendix 6 Control Effectiveness Rating Table

STEP 1: RISK IDENTIFICATION

The first step to conducting the Risk Assessment is to ask risk owners to validate the business objectives of that business area. Having validated the key objectives, the 'key' risks to achieving these objectives should be identified.

Risk identification is the process of identifying risks in the context you have established. The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. Risks represent areas of uncertainty in achieving objectives (i.e. 'what can go wrong' or 'what can happen'). 'Key' risks are managements' view of the most serious threats to the business objectives.

Risk Number (#) – Auto-generated for recording purposes.

Risk Name – Short title of the risk event.

Risk Event Description – Describe the risk event. What happens?

Sources of Risk and Impact – Describe factors that can cause the risk. How can the risk occur? What trigger the event? There may be multiple causes leading to a risk event. What is its impact/consequences? There may be multiple impacts (financial and non-financial) to a single event. To illustrate:

- A cause could be ineffective IT security,
- The event could be theft of customer data by an external party, and
- Consequences could be financial (high cost of repair /recovery of data) and/or non-financial (e.g. reputation).

Risk category - select the highest impact of a risk category for that event.

Risk Owner - A Risk Owner must also be assigned to each risk. The Risk Owner is the individual primarily responsible for identifying, assessing, managing and monitoring the risk.

STEP 2: CONTROL IDENTIFICATION AND ASSESSMENT

This step involves identifying and considering the current controls that are working effectively to mitigate the risk.

Risk Mitigation

Control Number (#) – Auto-generated for recording purposes.

Control Name – Short title of the control activity.

Current Controls Description – The controls should be adequately described so that someone unfamiliar with the business area processes can easily identify the applicable control. For example, if the control is described as segregation of duties, it may not be apparent what or who this relates to. A clearer description might be segregation of duties between function x and function y.

Control Owner - Each control should also be assigned a Control Owner. The Control Owner is the individual responsible for designing, maintaining and monitoring the control. The Control Owner may be from another business area.

Control Type – A mix of the control type should also be identified. Control type can be: Preventative, Detective and Mitigating.

Control Assessment (control design and control performance/Operating effectiveness) - The controls relating to each risk are collectively assessed based on design and performance by the Control Owner, in accordance with the tables in Appendix 6. This assesses the combined design and the combined performance of the controls in mitigating the risk. In determining this assessment, more weight may be placed on particular controls, given their role in managing a risk. The control design and control performance are combined to determine the overall control effectiveness.

STEP 3: RISK ANALYSIS & ASSESSMENT

Frequency/Likelihood - the estimated number of risk events in the next 12 months.

Consequences – Impact/Severity is assessed based on financial and non-financial impact. **Refer to** a four-level rating scale applies to each of these factors, as illustrated in **Appendix 4**.

Overall Control Effectiveness – The control design and control performance (or operating effectiveness) are combined to determine the overall control effectiveness in **Appendix 6**.

Risk Owner Response – Risk Owner must determine the appropriate response to the risk in **Appendix 5**. When determining the risk response, the risk assessment and risk appetite should be considered, i.e. if not within appetite, the response should be 'active management'.

Associate to objectives - Where practical, risks should be linked to a business objective. One objective could have more than one risk associated with it.

STEP 4: RISK TREATMENT

The purpose of risk treatment is to identify the most appropriate risk mitigation strategies and implement them. If the risk response for any of the identified risks is 'Consider control improvement', or 'Active management', an issue or action may be required. Where this is the case, the issue/action should be identified by the Risk Owner within or post-workshop. The issue/action should then be managed in accordance with the Issues and Actions Guidelines.

		Action Plan Report							
ssu	e								
ID	Name	Description	Deadline	Impact	Risk Rating	Issue Type	Linked Risk	Owner	
1									
A	ctions								
ID	Name	Description			Due Date	Remedial or Strategic	Status	Owner	
1	1								

Objective - The Issues and Actions process aims to:

- Promote the early identification of concerns, weaknesses or improvements to the risk and control environment, and
- Ensure proactive escalation and monitoring of issues and actions

Develop action plan

Issue Name - Title of issue.

Issue Description - Clear and concise description of the issue (described in a manner so it can be provided directly to the MANEX/Managers without further editing).

Issue Owner - All issues must be appointed an Issue Owner. The Issue Owner is the individual responsible for resolving the issue. The Issue Owner is typically the person responsible for the business area/function that is exposed to the risk that leads to the issue being raised and as such, is often the Risk Owner. The Issue Owner must be senior enough to drive outcomes.

Due Date - Due date for resolution of issue. Resolution dates should be sensible, realistic and reflect the Issue rating.

Issue Risk Rating - Rating an issue allows for prioritisation of action, i.e. higher rated issues should receive priority over lower rated issues. The issue rating also determines the escalation and oversight (Appendix 8) required.

Action Name- Title of action.

Action Description - Actions are identified for all Issues. Actions are essentially the tasks to resolve an issue. For example, if an issue is identified relating to the effectiveness of IT access controls, the actions may be 1) to review the access log and 2) to deactivate unused profiles.

Due Date - Set the due date to implement the action.

Action Owner – The Issue Owner is required to assign an Action Owner (Responsible Manager) for each action. The Action Owner is the individual responsible for ensuring appropriate closure of the action. Action Owners and the related Issue Owners are generally expected to be in a direct reporting line. If this is not the case, the Issue Owner must ensure they have agreement from the nominated Action Owner (and their manager if appropriate).

Appendix 8 – Risk Escalation Response

	Risk Actions and Escalation Points										
Group	Group Description	Action required for risk	Risk Escalation								
12-16	Red- Extreme	Action required: risks that cannot be accepted or tolerated and require treatment	Escalated to the MANEX Control strategy developed and monitored by MANEX								
5-11	Yellow- Moderate	Potential action: risks that will be treated as long as the costs do not outweigh the benefits As Low As Reasonably Practicable (ALARP)*	Managed at functional or service group level Escalated to the relevant direct report to MANEX for information								
1-4	1 - raan - 1 aw	No action: acceptable risks requiring no further treatment May only require periodic monitoring	No action required Monitoring within the functional area or business unit								

^{*} ALARP stands for 'As Low as Reasonably Practicable' refer to ISO 31010

RATING OF ISSUE

All issues must be rated in accordance with the Council Issue Rating table. Issues are rated based on financial and non-financial impact. Issues are assessed based on the *potential risk* to Council if the issue is not resolved.

Appendix 9 – Risk Management Activities

Action	Description	Responsibility	Timing
ERM Policy	Review the currency and effectiveness	Executive Manager, Governance; Review and approved by ARIC	Every two years
Risk Appetite Statement	Review the appropriateness for relevance and context	Executive Manager, Governance; Review and approved by ARIC	Annually in conjunction with the annual planning process
ERM Framework	Review the currency and effectiveness	Executive Manager, Governance; Review and approved by ARIC	Annually in December or after significant change
Business Unit Operational Risk Registers	Review risks and controls contained in Business Unit risk register and identify new or emerging risks	Business Unit Managers (risk owners) supported by Executive Manager, Governance	Six-monthly in conjunction with Business plan Review Process or when there is a material change
Strategic Risk Registers	Review risks and controls contained in Strategic risk register and identify new or emerging risks	MANEX supported by Executive Manager, Governance	Six-monthly in conjunction with Strategic plan Review Process
Issue & Action Plans	Ensure that actions required by Issue & Action Plans are incorporated into the Risk Dashboard Reporting. Actions are tracked to completion.	Business Unit Manager/Leaders, MANEX coordinated by Executive Manager, Governance	Quarterly in conjunction with Risk Reporting process
Risk assessments for major projects/ initiatives	Conduct risk assessments as required for major new or altered activities, processes or events	Relevant Manager/ Risk Owner, supported by Executive Manager, Governance	Prior to deciding to proceed with new project/initiative
Risk Dashboard reporting	Ensure that key risk information is contained in the risk dashboard to the MANEX, ARIC.	Executive Manager, Governance, reported to ARIC.	Quarterly
Training	Ensure risk owners and other staff are aware of the risk management process and their obligations	Executive Manager, Governance	Refresher for all Managers and Risk Owners every two years. Introduction for all new staff at induction.
Staff Performance Review	Ensure risk management performance of Risk Owners and people with responsibilities are assessed on a regular basis	Risk owners, MANEX, reported to ARIC	Annually

Action	Description	Responsibility	Timing
Communication	Ensure staff are aware of relevant risk management issues. Typical communication may include:	GM, supported by Executive Manager, Governance	Ongoing
	 Changes to related policies & procedures 		
	 Management response to recent issues & incidents 		
	 Benefits realised from risk management initiatives 		
	 Activities & alerts in staff newsletters and social media channels 		