RISK MANAGEMENT POLICY

June 2022

PREPARED BY:
CORPORATE GOVERNANCE UNIT

4-20 Eton Street,
Sutherland NSW 2232
T 02 9710 0333
sutherlandshire.nsw.gov.au

RISK MANAGEMENT POLICY

1. PURPOSE

The purpose of this policy is to outline Council's commitment to implementing organisation-wide risk management principles, systems and processes that ensure consistent, efficient and effective assessment of risk in all Council's planning, decision making and operational processes to assist Council achieve its objectives and commitment to the community, aligned with its Delivery Program and Operational Plan.

2. APPLICATION

The policy applies to all Councillors, Executive, managers, employees and contractors across all of Council's activities and processes.

3. PRINCIPLES

3.1. Application of Principles

No one principle should be applied to the detriment of another. Principles must be collectively considered and applied to the extent that is reasonable and practicable in the circumstances.

3.2 Principles

Principle	To achieve this, Council will:
A structured and tailored approach to the way risk is managed	• Adopt and implement a risk management framework, appropriate to Council's activities and operating environment, and consistent with the principles of *Australian Standard AS/NZS ISO 31000:2018 Risk Management* (outlined in Schedule A of this Policy). • Establish appropriate mechanisms for: ○ determining risk appetite and tolerance (outlined in Schedule B of this policy) ○ risk identification, assessment and management ○ measuring and reporting risk management performance, and ○ responding to deterioration in risk management performance and learning from incidents.

Principle	To achieve this, Council will:
Consistent, efficient and effective management of risk	• Seek to understand and manage the internal and external risks that may impact the delivery of Council's objectives and strategic goals through consideration of risk in four broad categories, as defined in section 10 of this document: ○ Strategic Risk ○ Business Risk ○ Project Risk ○ Enterprise Risk • Develop a consistent approach to risk assessment and mitigation. • Assign responsibilities to employees at all levels for the management of risk. • Embed key controls to manage risk into all levels of business processes and decision-making in accordance with Council's identified risk appetite.
Continual improvement in risk management	• Support a strong risk management culture through the development and implementation of: ○ a governance structure to oversight implementation of its risk management framework; ○ a risk management process; ○ supporting materials, and ○ a training and awareness program.

4. RESPONSIBILITIES

4.1 Council

Council is responsible for setting Council's risk appetite.

4.2 Audit, Risk and Improvement Committee

Council, with the assistance of the independent Audit, Risk and Improvement Committee provides oversight and assurance of the operational implementation of the Enterprise Risk Management Framework.

4.3 Chief Executive Officer

The Chief Executive Officer is responsible for leading development of risk management culture across the organisation and ensuring that this Policy is being effectively implemented.

4.4 Directors

Directors are responsible for ensuring their Directorate adheres to the requirements of this Policy and provide guidance in respect of risk management across the organisation.

4.5 Senior Managers

Senior Managers are the risk owners and are required to create an environment where the management of risk is accepted as the personal responsibility of all employees and contractors.

4.6 Employees

Employees are responsible and accountable for taking practical steps to minimise Council's exposure to risk so far as is reasonably practicable within their area of activity and responsibility.

5. POLICY COMPLIANCE

Ongoing, scheduled monitoring of the efficacy of the implementation of the Framework will be undertaken by the Enterprise Risk Management Committee on behalf of the Executive.

6. RECORD KEEPING, CONFIDENTIALITY AND PRIVACY

Council adheres to and complies with the NSW State Records Act 1998 and Privacy and Personal Information Protection Act 1998 through its Enterprise Content Management Policy and Privacy Policy.

7. BREACHES OF POLICY

Breaches of this policy will be dealt with in accordance with normal disciplinary procedures and may be advised to the CEO and or Director via the Manager.

8. RELATED DOCUMENTS

- Code of Conduct
- Fraud and Corruption Prevention Policy
- Public Interest Disclosure Policy
- Work, Health and Safety Management System

9. RELEVANT LEGISLATION, REGULATIONS AND GUIDELINES

- Local Government Act 1993 (NSW)
- State Records Act 1998 (NSW)

- Work Health and Safety Act 2011 (NSW)
- Work Health and Safety Regulation 2012 (NSW)
- Privacy and Personal Information Protection Act 1998 (NSW)
- Government Information (Public Access) Act 2009 (NSW)
- ISO 31000: 2018 Risk Management

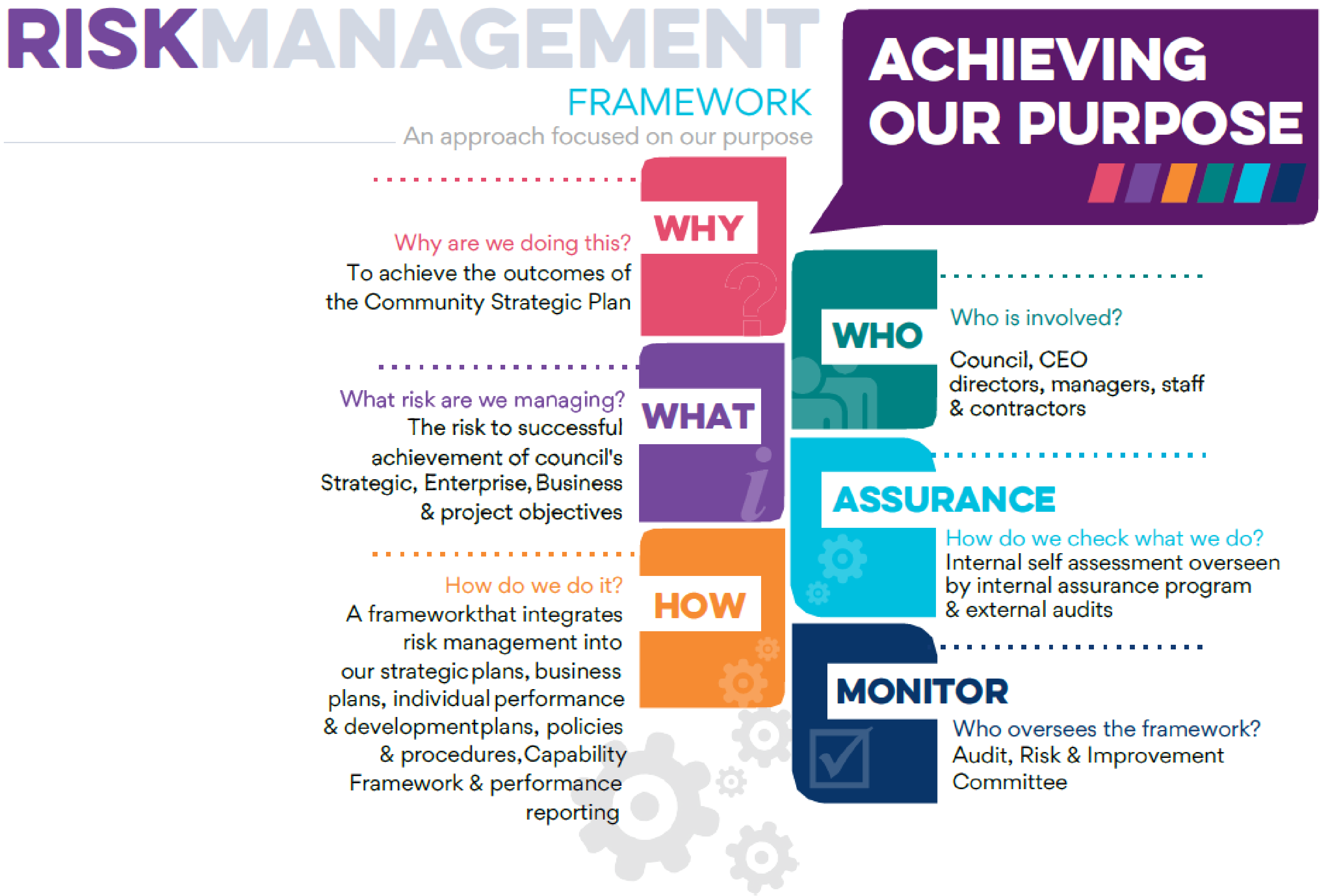
10. DEFINITION OF TERMS

Term	Meaning
Strategic Risk	Organisation wide risks which may impact on the organisation's ability to deliver on its community strategic plan or critical services.
Business Risk	Risk that is managed by Directorates and Senior Managers and consists of uncertainties associated with the successful achievement of Directorate and Division objectives.
Project Risk	Risk that is managed by Project Managers and consists of uncertainties associated with the successful achievement of project objectives.
Enterprise Risk	Risk that is managed by the Executive and consists of key enterprise-wide risks to the successful achievement of Council's objectives and outcomes. Key enterprise risks comprise of those strategic, business and project risks that have the potential to significantly affect the successful delivery of Council's objectives and outcomes.
Enterprise Risk Management	The set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.
Risk	The effect of uncertainty on the successful achievement of objectives.
Risk Appetite	The amount of risk that the organisation wants to take and is willing to accept in pursuit of its objectives.
Risk Management	Coordinated activities to direct and control an organisation with regard to risk.

End of document

<table>
<tr><td colspan="4"><b>UNCONTROLLED COPY WHEN PRINTED - For up to date copy please refer to Sutherland Shire Council Intranet / Website</b></td></tr>
<tr><td colspan="2"><b>Document Name</b>: Risk Management Policy</td><td colspan="2"><b>Policy Accountability</b> Manager Corporate Governance</td></tr>
<tr><td><b>Version:</b> 1.0</td><td><b>Approved by:</b> Corporate Governance Committee</td><td><b>Minute No</b>: 11 (GOV15-22)</td><td><b>Date approved</b>: 6 June 2022</td></tr>
<tr><td><b>Original:</b> June 2022</td><td><b>Last Revision</b>: N/A</td><td colspan="2"><b>Next Revision</b>: June 2026</td></tr>
</table>

SCHEDULE A
Enterprise Risk Management Framework



RISKMANAGEMENT FRAMEWORK

An approach focused on our purpose

ACHIEVING OUR PURPOSE

WHY

Why are we doing this?

To achieve the outcomes of the Community Strategic Plan

WHAT

What risk are we managing?

The risk to successful achievement of council's Strategic, Enterprise, Business & project objectives

HOW

How do we do it?

A frameworkthat integrates risk management into our strategicplans, business plans, individual performance & developmentplans, policies & procedures,Capability Framework & performance reporting

WHO

Who is involved?

Council, CEO directors, managers, staff & contractors

ASSURANCE

How do we check what we do?

Internal self assessment overseen by internal assurance program & external audits

MONITOR

Who oversees the framework?

Audit, Risk & Improvement Committee

SCHEDULE B
Enterprise Risk Appetite Statement

Risk Category	Risk Appetite Statement (Qualitative)	ACCEPT Risk Tolerance Statement (Quantitative) To achieve this, Council can tolerate:	RESIST Risk Tolerance Statement (Quantitative) In making decisions, Council has a low appetite for, and will attempt to resist:	AVOID Risk Tolerance Statement (Quantitative) In achieving its objectives, Council will not tolerate:	Risk Appetite Level Acceptable level of appetite, once reached it triggers the need for further considerations/ mitigations/ monitoring of the risk
Financial & Assets	Council will seek commercial and/or strategic opportunities but will always maintain a prudent financial management approach.	• Calculated financial risks in order to implement Council strategy including delivery of important infrastructure, improved service delivery, and the promotion of ecological sustainability. • Minor unforeseen and/or unavoidable cost variations up to 5% of business unit budget, as a result of a need to meet community needs or pursue commercial and/or strategic opportunities.	• Deviations from adopted Council Policy and Plans including Community Strategic Plan, Delivery Program, and Asset Management Plans and the objectives contained within. • Risks that will result in: - material anticipated budget variances; - the inefficient utilisation of Council assets; - impact service delivery to the community; - a detrimental impact to asset conditions; - a deferral of asset renewal investment.	• Risks that cause inaccurate reporting or breaches of: - statutory deadlines; or - due diligence in statutory planning; or - legislative approval on assets; or - against the law. • Breach of financial policies and delegations (e.g. Material misstatement in financial accounts) • Maladministration, misuse or waste of Council funds or resources. • Risk which may have a significant negative impact on Council's long term financial sustainability, are highly speculative, and are outside the LTFP parameters.	**Medium**
WHS/ Employee Safety	Council is committed to maintain the health and wellbeing of its workforce and to pursue opportunities to further improve it.	• Minor incidents or injuries/illnesses that occur in undertaking normal business activities despite best efforts to avoid or mitigate, provided we learn from them.	• Complacency in undertaking normal business activities	• Activities that result in reasonably foreseeable and preventable fatalities, harm, serious injuries or illnesses, serious near misses to staff, contractors and public. • Lost time injuries or notifiable incident/injury/illness. • Significant breaches of legal obligations. • Failure to learn from past incidents.	**Low**
Environmental	Council is committed to making decisions that promote ecologically sustainable development (activities).	• Minor and /or short-term environmental impact necessary in order to achieve key objectives • Minor environmental impacts (e.g. biological diversity and ecological integrity) from uncontrollable or unforeseen events. • Risks to the environment where any potential or actual damage can be repaired, offset or restored.	• Natural environmental damage arising from normal business activities.	• Risks which may have significant and/or long term negative environmental consequences or are highly speculative • Activities and practices that knowingly compromise the environment, are reasonably foreseeable and preventable.	**Medium**
Reputation	Council is committed to making decisions that	• Localised, short term negative publicity as a consequence of	• Entering into public debate on matters that are not areas of	• Negative publicity: - which is not objective/impartial or	**Medium**

SCHEDULE B
Enterprise Risk Appetite Statement

Risk Category	Risk Appetite Statement (Qualitative)	ACCEPT Risk Tolerance Statement (Quantitative) To achieve this, Council can tolerate:	RESIST Risk Tolerance Statement (Quantitative) In making decisions, Council has a low appetite for, and will attempt to resist:	AVOID Risk Tolerance Statement (Quantitative) In achieving its objectives, Council will not tolerate:	Risk Appetite Level Acceptable level of appetite, once reached it triggers the need for further considerations/ mitigations/ monitoring of the risk
	are in the best interests of the whole community and in line with our strategic objectives and accepts this may result in negative publicity or reputational damage as a consequence of competing stakeholder priorities and interests.	making decisions in the best interests of the broader community, in an environment where there are competing priorities and interests • Moderate level complaints associated with changes in policy from a changing political environment. • Isolated minor incidents, concerns and complaints that can either be resolved by day-to-day management, are assessed as not sufficiently damaging as to warrant the sustained efforts required to resolve them, or are incapable of being sufficiently resolved	Council responsibilities (other than to clarify roles/responsibility/lead agency) • Engaging in reactive communications, particularly on social media, where clear corporate communications are in place/been delivered, and there is limited possibility of resolving issue or perception	accurate, and damages Council's reputation; or - which is the result of inadequate planning and consultation with key stakeholder. - which is the result of mismanagement of all other risks as outlined here (or non-compliance)	
Legal /Liability	Council has an appetite for doing all that is reasonably practical with its limited resources to meet/comply with legal obligations.	• 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 or may occur from time-to-time, provided we learn from them.	• Litigation in favour of initiate contractual/legal disputes seeking a commercially pragmatic option when available	• Acting/Failure to Act which results in initiation of legal proceedings against Council or indictable offences against Council • Fraudulent, unethical and corrupt conduct. • Instances where Council Officials deliberately or recklessly break the law, fail to comply with legal obligations or deliberately or recklessly breach internal policies. • Significant breaches of legal obligations or contractual arrangements that result in fines, penalties or significant reputational damage.	**Medium**

SCHEDULE B
Enterprise Risk Appetite Statement

Service Delivery	Council is willing to transform and embed changes in many parts of business activities through lessons learnt, resilience developed, and innovations pivoted to support quality of life, liveable place and values in the community.	• Minor disruptions to critical Council services or short-term disruption to less critical services within council's Business Impact Analysis. • Business interruption in the short term where there is a demonstrable advantage in doing so. • Deviation from the Councils operational plan with appropriate authorisation that will achieve benefit to Council.		• Risks that may severely disrupt Council's ability to conduct core daily activities/services • Risks that cause inaccurate reporting or breaches of Statutory deadlines or due diligence in Statutory planning and legislative approval on assets • Risks that disrupt any Council critical services beyond 3 days and other less critical services as per Council established maximum tolerable outages per Council BCP	**Medium**
Community / Public health & Safety	Council will do all that is reasonably practical to provide agreed services & agreed service levels, and where necessary will priorities those services that maintain the health and safety of the public.	• Risks that result in some inconvenience to the community that is necessary in order to achieve key public safety objectives. • When faced with competing demands we will prioritise services that protect and enhance the health and safety of our community	• Deviations from agreed service levels	• Risks that severely impact public property safety and/or severely impact public health • Risks that impact public safety due to poor practices of contractors • Asset infrastructure that does not meet standard within the processes of renewal or upgrade Risks that leave public asset/infrastructure in an unsafe situation • A failure to respond in an agreed timeframe to reported defects of Council assets	**Low**
Information, Security and Technology	Council will pursue innovative opportunities to transform its digital services whilst maintaining security and privacy as paramount	• Minor downtime or outage in a single area that is incidental to normal business operations/activities despite best efforts to avoid or mitigate, provided we learn from them. • Unforeseen interruptions from uncontrollable events of up to 3 days where council responds and communicates promptly to impacted stakeholders. • Minor impacts to service delivery issues due to operational impacts with A critical systems availability of at least 95% • Agile ways of working within adopted/agreed Framework	• Departure from agreed processes e.g. Data leakage • Shadow IT Programs • Bespoke system configurations • Customisation of solutions /third party products where there is no approved business Case	• 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 threaten council IMT security and privacy on customer data • Any vendors who do not meet Council's established security standards and or IOS standards • Off-shore hosting/storage of personal data • On premises infrastructure, increasing the number of supported, adopting applications, services or architecture that would reduce our security posture	**Medium**

SCHEDULE C
Enterprise Risk Matrix Ranking Tool

CONSEQUENCE									LIKELIHOOD When we look at ‘**Likelihood**’, we are looking to identify the frequency or probability chance of the particular risk occurring. We are required to determine the most appropriate rating depending on the description.				
Financial & Assets	**WHS**	**Environment**	**Reputation**	**Legal Liability**	**Service Delivery**	**Community Wellbeing & Safety**	**Information Security & Technology**	**Descriptor**	**Rare** Unforeseeable or may occur in exceptional circumstances	**Unlikely** Could happen but probably won't	**Possible** Might occur at some time but not supported by data	**Likely** Experience / data suggests comparable events have occurred	**Almost Certain** Experience / data strongly suggests it will happen
Extensive financial or asset loss of > 1M or > 50% of revenue	Extensive multiple casualties or multiple fatalities	Extensive irreparable damage	Extensive public outcry. Potential International media attention.	Extensive litigation or indictable offence	Loss of a *Critical Service >1 month that may impact community safety	Extensive multiple casualties or multiple fatalities	Irretrievable loss of critical data	**Catastrophic**	**Medium (8)**	**High (16)**	**Extreme (20)**	**Extreme (23)**	**Extreme (25)**
Major financial or asset loss of 500k to 1M or up to 50% of revenue	Major casualty or single fatality	Localised irreparable damage	Major public outcry. Potential national media attention.	Major litigation, claim or prosecution	Loss of a *Critical Service > 2 weeks Non-critical service >1 Month	Major casualty or single fatality	Loss of critical IT services >2 weeks	**Major**	**Medium (7)**	**Medium (12)**	**High (17)**	**Extreme (21)**	**Extreme (24)**
Significant financial or asset loss of 50k to 500k or up to 25% of revenue	Moderate injury/illness requiring hospitalisation	Major damage requiring remediation	Serious public outcry. State media attention	Litigation, significant claim or fine	Loss of a *Critical Service < 2 weeks Non-critical service <1 Month	Moderate injury/illness requiring hospitalisation	Loss of critical IT services < 2 weeks	**Moderate**	**Low (4)**	**Medium (10)**	**High (15)**	**High (18)**	**Extreme (22)**
Minor financial or asset loss of 25k to 50k or up to 15% of revenue	Minor injury/illness requiring treatment by doctor	Moderate adverse effect requiring clean up	Significant community concern with local media attention.	Moderate claim or fine	Loss of a *Critical Service < 1 weeks Non-critical service <2 weeks	Minor injury/illness requiring treatment by doctor	Loss of critical IT services < 1 weeks	**Minor**	**Low (2)**	**Low (5)**	**Medium (11)**	**High (13)**	**High (19)**
Negligible financial or asset loss of <25k or <10% of revenue	Insignificant injury/illness requiring first aid treatment	Minor adverse effect with limited clean up	Heightened local community concerns and criticism	Minor claim, fine or action with short term significance	Loss of a *Critical Service < 1 day Non-critical service <1 weeks	Insignificant injury/illness requiring first aid treatment	Loss of critical IT services < 1 day	**Insignificant**	**Low (1)**	**Low (3)**	**Low (6)**	**Medium (9)**	**High (14)**

* **Critical services** are services that support the minimisation of harm to human health & the environment & the internal support services they depend on.

Risk Appetite Statement (RAS) the acceptable level of appetite for each risk category, once reached it triggers the need for further considerations/ mitigations/ monitoring of the risk

Medium Financial & Assets	**Low** WHS	**Medium** Environment	**Medium** Reputation	**Medium** Legal Liability	**Medium** Service Delivery	**Low** Community Safety	**Medium** IST

SCHEDULE C
Enterprise Risk Matrix Ranking Tool

End of Document

<table>
<tr><td colspan="4"><b>UNCONTROLLED COPY WHEN PRINTED -</b> For up to date copy please refer to Sutherland Shire Council Intranet / Website</td></tr>
<tr><td colspan="2"><b>Document Name</b>: Schedules to Risk Management Policy</td><td colspan="2"><b>Schedule Accountability</b>: Manager Corporate Governance</td></tr>
<tr><td><b>Version</b>: 1.1</td><td><b>Approved by</b>: Corporate Governance Committee</td><td><b>Minute No.</b> 11 (GOV15-22)</td><td><b>Date approved:</b> 6 June 2022</td></tr>
<tr><td colspan="2"><b>Original:</b> June 2022</td><td><b>Last Revision</b>: December 2024 (Administrative)</td><td><b>Next Revision</b>: June 2026</td></tr>
</table>