ENTERPRISE RISK MANAGEMENT FRAMEWORK P3.0395.1

www.camden.nsw.gov.au

ENTERPRISE RISK MANAGEMENT FRAMEWORK

DIRECTORATE: Customer and Corporate Strategy

BRANCH: Safety and Risk

CATEGORY: 1

Table of Contents

1. Introduction

This Enterprise Risk Management (ERM) Framework provides a structure and criteria for sound and consistent risk management decisions across a broad range of context and circumstances in a diverse and complex organisation.

The Framework enables Camden Council (Council) to operate within acceptable risk parameters and supports the Enterprise Risk Management Policy by describing the system and the criteria used for the evaluation and management of risk.

The Framework aligns with ISO 31000:2018 and complies with NSW Office of Local Government (OLG) Guidelines on Risk Management and Internal Audit for Local Government.

2. ERM System Structure

The ERM system encompasses the following components:

- Enterprise Risk Management Policy
- Enterprise Risk Management Strategy 2024-2027
- Enterprise Risk Management Framework
- Enterprise Risk Management Procedures (Strategic, Operational and Project)
- Enterprise Risk Management information system and reporting

3. Types of Risk

This ERM Framework deals with the following types of risk:

Strategic Risks	Threats and uncertainties that could affect the achievement of Council's strategic objectives. These risks arise from factors within the organisation's control (e.g. operational inefficiencies, succession planning, resource constraints) and external factors beyond its influence (e.g. regulatory changes, economic instability, community expectations, social dynamics).
Operational Risks	Threats and uncertainties inherent in the day-to-day activities Council performs when delivering its services and functions.
Project Risks	Threats and uncertainties that could affect the delivery of a project.

4. Three Lines of Defence

The ERM system incorporates the principle of the 'Three Lines of Defence' for increased reliability in managing risk exposures.

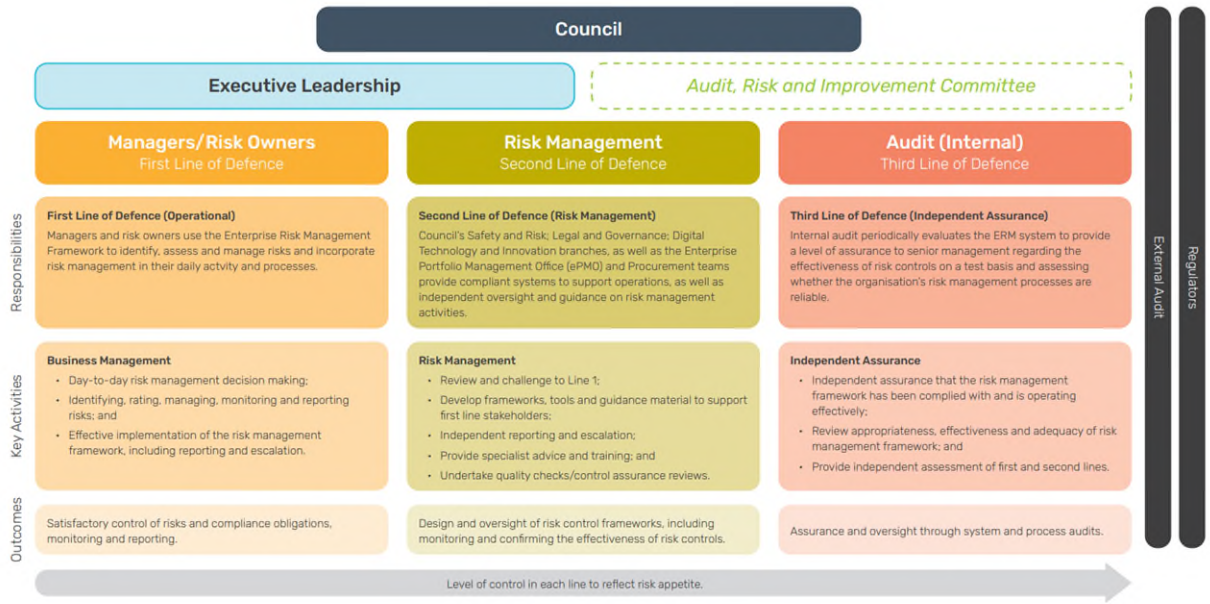

Figure 1: Three Lines of Defence Model

1. First Line of Defence (Operations)

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

2. Second Line of Defence (Risk Management)

Council's Safety and Risk; Legal and Governance; and Digital Technology & Innovation branches, and enterprise Portfolio Management Office (ePMO) provide compliant systems to support operations, as well as independent oversight and guidance on risk management activities.

3. Third Line of Defence (Internal Audit)

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

5. When is a Risk Assessment Required?

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

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

6. Risk Assessment Process

Council follows a standard risk management process consistent with ISO 31000:2018, which is detailed in the associated ERM processes.

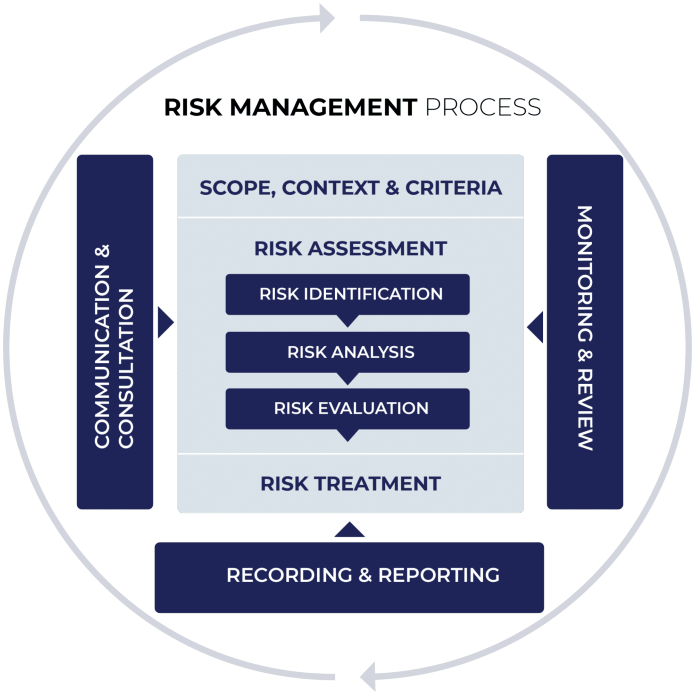

Figure 2: IS031000:2018 Risk Management Process

7. Risk Categories

The following risk categories apply across Strategic, Operational, and Project risks and provide guidance for identifying and categorising potential risk exposures.

These risk categories correspond to the consequence descriptors in Table 4.

Risk Category	General Guidance Description (includes but not limited to)
Safety	- Work Health & Safety - Personal Injury - Psychosocial
Financial	- Economic (inflation/deflation) - Finances (cash flow) - Fraud / Theft - Interest Rates - Litigation
Service Delivery	- Asset Management - Business Disruption - Information Communication Technology (ICT) Management - Economic / Business Development - Human Resources
Regulatory	- Governance - Legislative and Regulatory Compliance - Contractor Management - Onboarding and Training - Policy and Procedures
Reputation	- Corporate Values - Customer Feedback - Media Coverage - Political - Wastage - Corruption
Environment	- Climate Change - Loss of Biodiversity - Natural Hazards - Public Health - Water
Project Delivery	- Project Budgets - Project Schedule - Project Outcomes and Benefits
Information/Cyber Security	- Personally Identifiable Information (PII) - Personal Health Information (PHI) - Confidential Information - Sensitive Data - Cyber Security

8. Criteria for the Assessment of Risk

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

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

Likelihood	Description	Quantification
Rare	The event may occur but only in exceptional circumstances. No past event history.	Once every 50 years or more.
Unlikely	The event could occur in some circumstances. No past event history.	Once every 20 years.
Possible	The event may occur sometime. There have been warning signs the event might occur.	Once every 5 years.
Likely	The event will probably occur. The event has occurred occasionally in the past.	Once a year.
Almost Certain	The event is expected to occur in normal circumstances. The event has occurred frequently in the past.	Several times a year.

'Consequence' is a semi-quantitative assessment of the potential impact or magnitude of the risk by reference to the descriptors in Table 4. For accuracy and consistency, it is essential to determine the 'worst credible outcome' if the risk were to occur, rather than the 'worst possible outcome'.

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

Risk Rating Matrix					
	Consequence				
Likelihood	5 Minimal	4 Minor	3 Moderate	2 Major	1 Severe
A Almost Certain	Medium	High	High	Very High	Very High
B Likely	Medium	Medium	High	High	Very High
C Possible	Low	Medium	Medium	High	High
D Unlikely	Low	Low	Medium	Medium	High
E Rare	Low	Low	Low	Medium	Medium

Figure 3: Risk Rating Matrix

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

Table 4: Consequence Descriptors

	Minimal	Minor	Moderate	Major	Severe
Safety	Incident and/or 'near-miss' with low potential for harm	Minor injuries or illness treated by first aid, that do not result in claims	Short duration lost time injury requiring minor medical treatment, minor breach of WHS legislation, multiple claims under excess	One off major breach of WHS legislation, lost time injuries requiring major medical treatment, large claims above excess	Loss of life or serious permanent injury, major prosecution for breach of WHS legislation, class action against Council
Financial	Negligible Financial Loss relative to the circumstances **Strategic Risk** financial losses: *<$50K* **Operational Risk** *<5% of budget*	Minor Financial Loss relative to the circumstances (not covered by insurance) **Strategic Risk** financial losses: *$50K-$100K* **Operational Risk** financial losses: *> 5-10% of budget*	Significant Financial Loss relative to the circumstances (not covered by insurance) **Strategic Risk** financial losses: *$100K-$500K* **Operational Risk** financial losses: *>10-25% of budget*	Major Financial Loss relative to the circumstances (not covered by insurance) **Strategic Risk** financial losses: *$500K-$1 million* **Operational Risk** >25-50% of budget	Extensive Financial Loss relative to the circumstances (not covered by insurance) **Strategic Risk** financial losses: *> $1 million.* **Operational Risk** >50% of budget
Service Delivery	Usual scheduled interruptions, unscheduled interruptions for less than 1 day Little or no impact on business objectives	Short term disruption to services for 1 to 3 days Some reprioritisations of resources to enable business objectives to be achieved	Inability to deliver critical programs and/or services for 3 days to 2 weeks Some important business objectives can no longer be achieved	Inability to deliver critical programs and/or services for 2 to 4 weeks A number of significant business objectives can no longer be achieved	Inability to deliver critical programs and/or services for >4 weeks Most objectives can no longer be achieved. Complete revision of long-term business model required.

Regulatory		Minor non-compliance not resulting in any action	Investigation finding technical breach of legislation	Minor breach of legislation resulting in warnings, improvement notices etc	Major breach leading to Investigation by external agency resulting in negative findings, fines or penalties	Significant breach leading to investigation by external agency resulting in successful prosecution or sacking of Council
Reputation		One off insignificant adverse local media or complaint	Heightened concerns from individual stakeholders, some short-term media concern	Concerns from some key stakeholders, major local media coverage (short duration)	Significant adverse media at state level, isolated loss of stakeholder trust, damage to rep. that takes many months to repair	Sustained negative national media coverage, total loss of stakeholder trust in Council, damage to reputation that takes many years to repair
Environment		Minor effects on built & natural environment, breach of guidelines, perception of damage	Short term effects on built & natural environment, damage to a single property or parcel of land, breach of policy	Serious medium-term effects on built & natural environment from single incident (e.g. one-off pollution spill)	Significant long-term impact on built & natural environment, investigation of Council with adverse findings	Very serious irreversible damage to environment and/or multiple sites or ecosystems, prosecution of Council.
Project Delivery	**Project Resources (Internal and External)**	Project resourcing (capacity and skill set) is sufficient to deliver the project	Project resourcing (capacity and skill set) is sufficient to deliver the project	Project is not suitably resourced (capacity and skill set) causing a minor impact on project delivery; can be managed within the confines of the project team (including Sponsor & Client)	Project is not suitably resourced (capacity and skill set) causing a tangible impact on project delivery; requires reporting to Directorate &/or ePMO Governance Committees	Project is not suitably resourced (capacity and skill set) causing a significant impact on expected project delivery; requires reporting to Directorate &/or ePMO Governance Committees
	Financial (Project Costs)	Project forecast financial losses (including contingency) <$50k	Project forecast financial losses (including contingency) $50K-$100K	Project forecast financial losses (including contingency) $100K-$500K	Project forecast financial losses (including contingency) $500K-$1 million	Project forecast financial losses (including contingency) >$1 million

	Project Delivery (Schedule)	Critical milestones and overall project schedule delayed up to <10 days or <5% of schedule, whichever is the greater	Critical milestones and overall project schedule delayed >10 days & <1 month or <10% of schedule, whichever is the greater	Critical milestones and overall project schedule delayed >1 month & <3 month or <20% of schedule, whichever is greater	Critical milestones and overall project schedule delayed >3 & <6 months or <30% of schedule, whichever is greater	Critical milestones and overall project schedule delayed >6 months or >30% of schedule, whichever is greater
	Project Outcomes & Benefits	No impact to business case and outcomes/benefits	No impact to business case and outcomes/benefits	Minor impact on business case and outcomes/benefits which can be managed within the confines of the project team (including Sponsor & Client)	Tangible impact on business case and outcomes/benefits which requires reporting to Directorate & ePMO Governance Committees	Significant impact on business case and outcomes/benefits which requires reporting to Directorate & ePMO Governance Committees and Council. Immediate assessment of project viability may need to be considered
Information/Cyber Security	**PII, PHI and Sensitive Information**	No sensitive information exposed Negligible disruption, No Impact, No regulatory violation, No or minimal financial loss	Small amount of non-critical PII or PHI exposed Minor disruption quickly resolved, Minimal negative attention, Minor breach, may require notification, Low financial cost.	Moderate amount of sensitive information exposed. Noticeable disruption requires effort, Moderate negative attention, potential media. Reportable breach, regulatory implications, potential investigations, Moderate financial cost, including fines and legal fees	Significant amount of sensitive information exposed. Major disruption, significant effort. Major negative attention, extensive media. Serious breach, significant regulatory implications. High financial cost, substantial fines and legal fees.	Extensive exposure, very large number of individuals affected. Severe and prolonged disruption. Severe damage, widespread media, loss of trust. Severe breach, extensive regulatory consequences. Extremely high financial cost, significant fines, and potential business loss.

	Non-Critical Systems	No impact on non-critical systems. Negligible disruption, No impact. No regulatory violation. No or minimal financial loss.	Minor performance issues in non-critical systems, quickly resolved Minor disruption quickly resolved. Minimal negative attention. Minor breach may require notification. Low financial cost	Moderate performance degradation, some user impact. Noticeable disruption requires effort. Moderate negative attention, potential media, Reportable breach, regulatory implications, potential investigations. Moderate financial cost, including fines and legal fees.	Major disruption, significant effort. Major negative attention, extensive media. Serious breach, significant regulatory implications. High financial cost, substantial fines and legal fees.	Severe and prolonged disruption. Severe damage, widespread media, loss of trust. Severe breach, extensive regulatory consequences. Extremely high financial cost, significant fines, and potential business loss.
	Critical Systems	No impact on critical systems Negligible disruption, No impact. No regulatory violation. No or minimal financial loss.	Minor performance issues in critical systems, quickly resolved. Minor disruption quickly resolved. Minor breach may require notification. Low financial cost.	Moderate performance degradation, some user impact. Noticeable disruption requires effort. Moderate negative attention, potential media. Reportable breach, regulatory implications, potential investigations. Moderate financial cost, including fines and legal fees	Significant system downtime, major user impact. Major disruption, significant effort. Major negative attention, extensive media. Serious breach, significant regulatory implications. High financial cost, substantial fines and legal fees	Complete system failure, critical operations halted. Severe and prolonged disruption. Severe damage, widespread media, loss of trust. s Severe breach, extensive regulatory consequences. Extremely high financial cost, significant fines, and potential business loss.

Table 4: Consequence Descriptors

9. Risk Appetite

Risk appetite criteria determines the acceptability of risks based on the level and type of risk the Council is willing to accept in line with its objectives, values, culture, and external factors.

Council's overall risk appetite is **Limited appetite (Guarded & Open)**

However, Council will always take a considered approach, choosing options that encourage the ability to innovate where risks are known to achieve strategic objectives and quality community outcomes. Council will always have no appetite for risk when it comes to safety.

		Risk Appetite			
		No appetite	**Limited appetite**	**Balanced appetite**	**High appetite**
		Averse Preference for options that avoid risk	Guarded & Open Willing to consider options. Preference for safe options with low degree of residual risk and an acceptable level of reward	Eager for Risk Enthusiasm for innovation leading to preference for higher rewards despite greater inherent risk	
Safety		X			
Financial			X		
Service Delivery			X		
Regulatory			X		
Reputation			X		
Environment			X		
Project Delivery				X	
Information / Cyber Security	*PII, PHI and Sensitive Information*	X			
	Non-Critical Systems			X	
	Critical Systems		X		

Table 5: Risk Appetite

It is acknowledged that some risks may be unable to be brought within appetite. When a risk assessment has determined that the level of residual risk is above the relevant risk appetite defined in Table 5 below, and it is not possible or practicable to implement controls that will bring a risk level within appetite, the General Manager and Directors have the authority to accept operations at risk levels above appetite if it is considered appropriate for the circumstances. It is the responsibility of the risk owner to complete the Above Appetite Checklist and provide these details to the relevant Director to factor into their consideration as to how to proceed.

10. Risk Treatment

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

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

11. System Evaluation and Continuous Improvement

In addition to an annual self-assessment, the ERM Strategy drives continuous improvement of the ERM system and culture. The following performance measures also contribute to continuous improvement by providing data on ERM performance.

Performance Measure	Criteria	Target
Risk Review	Branch managers actively participate in twice-yearly service based operational risk reviews within allocated three-month review period	80%
Risk Appetite	Reduction in number of risk rating levels that exceed risk appetite from one reporting period to the next (6 monthly)	Downward trend
Risk Treatment	Completion of risk treatment actions by due date	80%
Stakeholder Satisfaction	Annual survey of satisfaction with risk management support service	80%
ERM Strategy Actions	Completion of Action Plan items by due date	80%
Reporting	All scheduled ERM reports to ELG and ARIC are completed on time with accurate and up-to-date information	100%
Training and Awareness	Completion/attendance rate for risk management training and awareness programs delivered to Council staff	50% - non mandatory, 90% mandatory
Risk Culture and Maturity	Alternating annual assessment of risk maturity and risk culture to determine if risk management practices have advanced	Upward trend; increase in positive results

12. Reporting

The ERM function has the following reporting requirements:

Report Type	Frequency	Reporting to
Reporting on implementation of the ERM Strategy and ERM performance measures	Quarterly	GM ELG ARIC
ERM Annual Self-Assessment	Annually	General Manager (GM) Executive Leadership Group (ELG) Audit Risk and Improvement Committee (ARIC)
Independent strategic assessment	Every four years	ARIC
Ad hoc reporting	As required	As required

In addition, reports to Council and ELG should include commentary on the risk implications of the matter being reported.

13. ERM Tools and Resources

Forms, Templates & Systems	Explanation
Enterprise Risk Assessment	Template for structuring a risk assessment. Includes Above Appetite Checklist
ERM Intranet Page	Source of ERM information, tools and resources
CAMMS	System that houses ERM information and actions
WHS Risk Management Procedure	Guidance on managing safety risks in compliance with WHS legislation
Project Management Framework	Source of project governance, tools and guidelines

14. References

- Enterprise Risk Management Policy
- International Standard ISO 31000:2018 Risk Management – Guidelines
- Local Government Act 1993 (NSW)
- Local Government (General) Regulation 2021
- NSW Office of Local Government Guidelines on Risk Management and Internal Audit for Local Government

Approval and Review	
Responsible Branch	Safety and Risk
Responsible Manager	Manager Safety and Risk
Date Adopted	Council – 11/03/2025
Version	1
EDMS Reference	25/136894
Date of Next Review	31/03/2025

Version Control				
Version	**Date Adopted**	**Approved By**	**EDMS Ref.**	**Description**
1	11/03/2025	Council	25/136894	Initial adoption of policy.

camden council

70 Central Avenue
Oran Park NSW 2570

13 22 63

mail@camden.nsw.gov.au

PO Box 183, Camden NSW 2570

www.camden.nsw.gov.au