Enterprise Risk Management Process

Policy Type	Council Process	Version:	3
Responsible Officer	Manager Development and Governance	Date Approved:	19/06/2024
Review Officer:	Director Corporate and Community Services	Review Due:	19/05/2026
Author:	Manager Development and Governance	Commencement:	19/06/2024

1. COUNCILS APPROACH

To manage all business risk, Council will follow the current published Australian Standard for risk management.[1] Using this approach there are six key stages to the risk management process.[2]

STEP 1. Communicate and Consult - with internal and external stakeholders

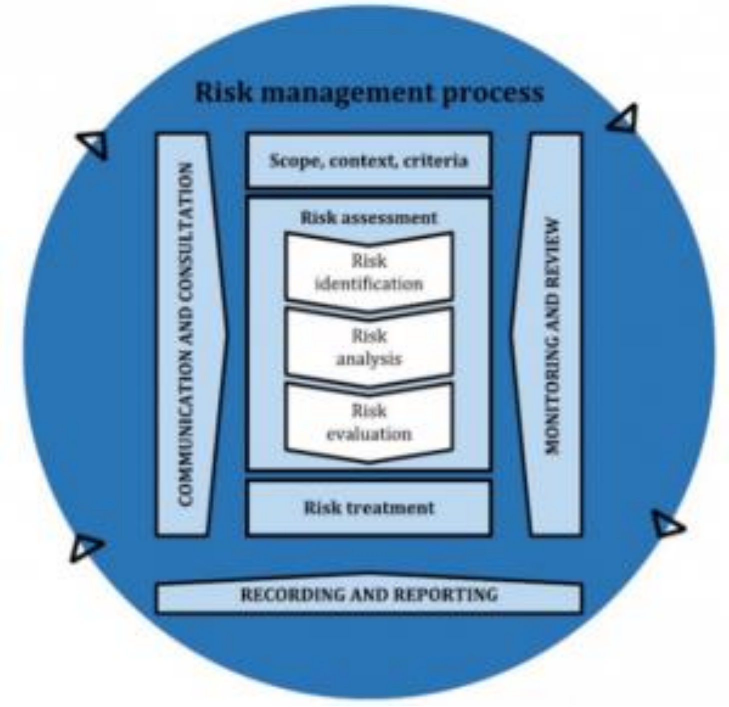
STEP 2. Establish the Context - the boundaries

STEP 3. Risk Assessment - identify, analyse and evaluate risks

STEP 4. Treat Risks - Implement and assess controls to address risk

STEP 5. Monitoring and Review - risk reviews and audit

STEP 6. Recording and Reporting - communicate outcomes



Our Risk Approach using AS/NZS ISO 31000:2018

[1] See *Australian Standard AS ISO 31000:2018 Risk management - Guidelines.*

[2] Ibid s 6.

2. COMMUNICATE AND CONSULT

Communication and consultation are integral to the process and must occur throughout the process. Communication efforts with stakeholders must be focused on two-way dialogue rather than a one-way flow of information from decision makers to stakeholders.

An expert's perception may differ from that of the layman's however both perspectives may contribute to the process. To limit ambiguity and duplication, risk assessments and treatments should be undertaken in a group environment with key stakeholders in attendance. Any uncertainties should be discussed to determine basic assumptions, measurements and mitigation strategies.

It is important to communicate and consult with stakeholders at each step of the risk management process. Communication efforts must be focused on consultation and two-way dialogue, rather than a one-way flow of information from decision makers to stakeholders.

The Manager Development & Governance will be available to assist employees throughout the risk management process including risk assessments, developing treatments and reporting.

Any changes to the Enterprise Risk Management (ERM) Framework that impact the process are to be communicated to all stakeholders.

3. ESTABLISH THE CONTEXT

This step provides value to the process as it is where the alignment, planning, understanding and preparation occur. The context concerns the understanding of the local government's scope for risk management and defines the criteria against which risks will be assessed. It also reviews any factors which may contribute or have a significant impact on the local government achieving its objectives.

It concerns the operations and activities of local government and reviews the internal and external environment in which these operations and activities operate. The context internal or external refers to the environment in which council seeks to achieve the particular objective being assessed this includes:

External context

- The cultural, social, political, legal, regulatory, financial, technological, economic and natural environment. (This can be local, state, national or international)
- Key drivers and trends having impact on council's objectives; and
- Relationships with, and perceptions and value, of external stakeholders.

Internal context

- Governance, organisational structure, roles and responsibilities;
- Corporate and operational plans, policies and objectives, and the strategies in place to achieve them;
- Organisational capabilities, in terms or resources, knowledge, systems and technology
- Relationships with, and perception and values of internal stakeholders; and
- Information systems and decision-making processes.

The risk management context considers the goals, objectives, strategies, scope and parameters of Council activities that could be a source of uncertainty or those parts of Council where the risk management process is being applied. This includes consideration of the benefits, costs and opportunities of risk management activities and the resources required. Setting the risk criteria is also part of establishing the context.

4. RISK ASSESSMENT

Risk Assessment is the overall process of risk identification, analysis and evaluation. The ERM Process details the risk assessment and treatment process and includes;

- Risk calculator
- Associated risk consequence and likelihood matrix tables
- Guidance on control and treatment plans

4.1 RISK IDENTIFICATION

Risk identification is the process of identifying key risks facing Council. This involves thinking through the sources of risks, the potential hazards, the possible causes and the potential exposure. If a risk is identified that the likelihood of occurring is within 3 months, then Managers should immediately do a risk assessment and treatment plan if required to be presented in Council's ordinary meeting.

Risk identification occurs within the context of the risk management activity, procedure or process. Council focuses on effective management of the following material risks categories and types:

Risk Category	**Risk Type**
Financial	Strategic Risk
Environmental	Financial Risk
Infrastructure and Assets	Operational Risk
Political and reputational	Information Technology
Legal, compliance	Human Resources
Health and Safety	Regulatory
Service Delivery and IT	Macro Risk

It is important to undertake a systematic and comprehensive identification of key risks. Quarterly the Risk Matrix will be updated with identified Risks during the previous quarter operations. The questions when identifying risks are:

- What can happen?
- Where can it happen?
- Why can it happen?
- How can it happen?
- What is the impact?
- When can it happen?

It is also important to consider the potential causes of a risk as it will help to address the risk, which is the next stage of the risk management process. Potential causes may include: commercial relationships, financial activities, operational issues, political influences, personal/human behaviour, natural events, business interruption, management activities, technology issues, technical issues or legal relationships.

A comprehensive list of risks is generated based on events that may create, enhance, prevent, degrade, accelerate or delay the achievement of Council's objectives. The identification activity should also include risk associated with not pursuing an opportunity as well as any risks not under Council's control.

Generally, risk identification and analysis tend to focus on the negative consequences of risk, and the consequence table normally reflects the negative or detrimental impacts. However, the risk management approach can be used to identify and prioritise opportunities with positive or beneficial consequences to enhance decision making and the achievement of objectives.

4.2 RISK ANALYSIS

Once identified, the risks can then be analysed. Risk analysis is a process using predetermined criteria to assess the level of risk based on the likelihood and consequences of a risk eventuating. From this analysis the level of inherent risk can be determined using the Risk Rating Matrix.

The methodology to analyse risks involves 4 steps;

Identify the existing controls - the controls that are currently in place to reduce the risk must be considered. Controls can include any policy, process, procedure, mechanism, practice or other actions which modify the consequences and/or their likelihood.

Rate the likelihood - likelihood is the chance of the consequence eventuating. The likelihood ratings ranging from 1 to 5 (rare to almost certain), located in the risk calculator, are used when considering the likelihood of a risk consequence eventuating.

Rate the consequences - the consequences reflect the extent of the impact on objectives. The consequences are considered in the context of the listed consequence categories, and the most likely severity or degree of each consequence. Consequence ratings from 1 to 5 (insignificant to catastrophic) are used when considering the range of impacts on Council and the Community. The greater the significance of the consequences on Council and the community, the higher the rating.

Determine the level of Risk - the combination of consequence and likelihood will produce a level of risk using the risk calculator. The severity ranges from low and moderate to significant and extreme.

Likelihood Matrix

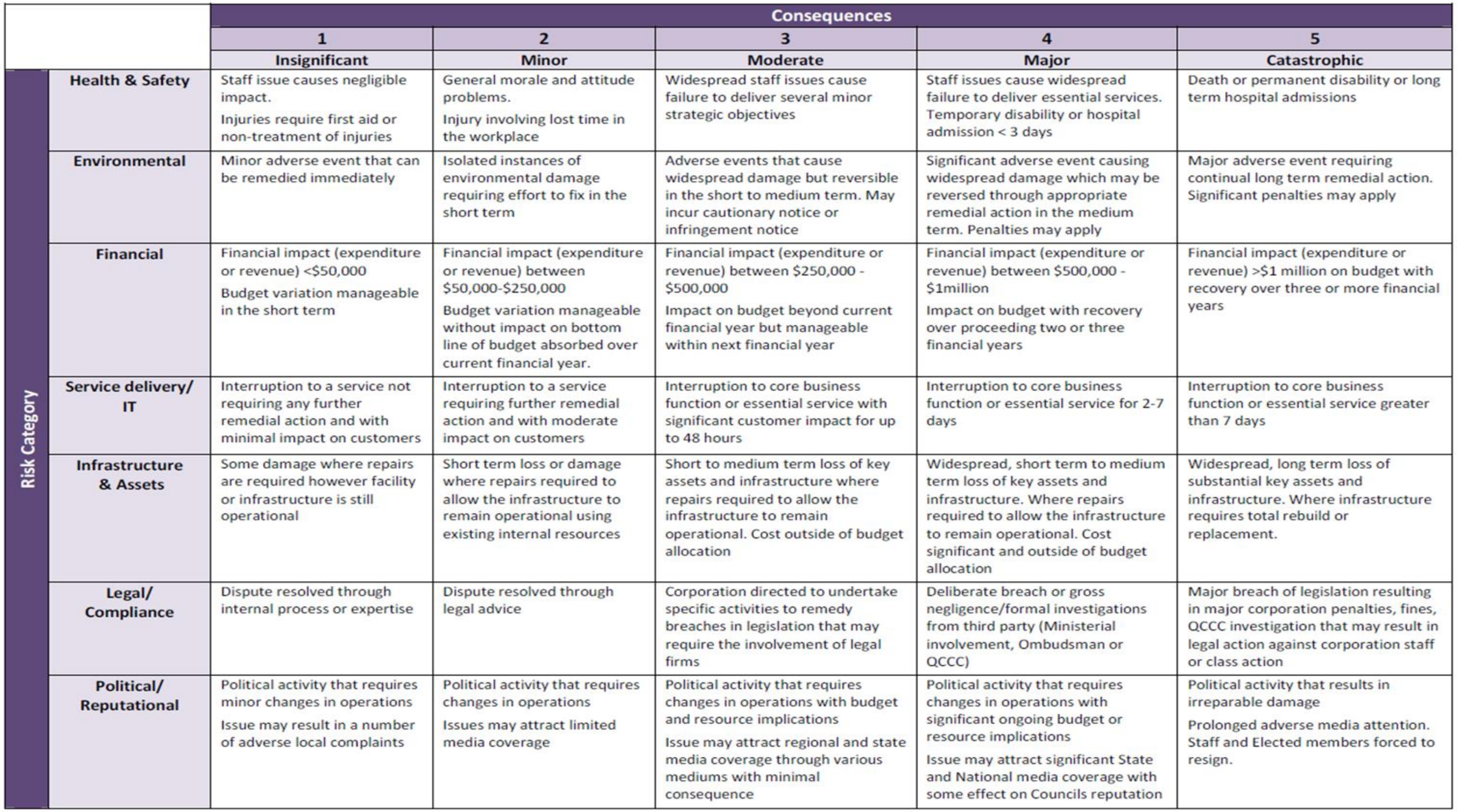
When considering the likelihood of a risk, you need to consider both the probability and frequency of occurrence. Council will use the following likelihood ratings:

Rating	Likelihood	Description	Quantification
1	Rare	The event may occur but only in exceptional circumstances. No past event history	Once every 50 years
2	Unlikely	The event could occur in some circumstances. No event history.	Once every 20 years
3	Possible	The event may occur at some time. Some past warning signs or previous event history	Once every 5 years
4	Likely	The event will probably occur. Some recurring past event history.	Once a year
5	Almost Certain	The event is expected to occur in normal circumstances. There has been frequent past history	Once every 6 months or more

Consequence Matrix

The consequence assessment is the effect or the impact of the risk event. It can be measured in a number of ways, such as financially (in terms of profit or loss), environmentally (in terms of effort required to remedy) etc. Council will utilise the following consequence ratings, based on the seven listed material risks.

Risk Consequence Matrix



		Consequences				
		1	2	3	4	5
		Insignificant	Minor	Moderate	Major	Catastrophic
Risk Category	Health & Safety	Staff issue causes negligible impact. Injuries require first aid or non-treatment of injuries	General morale and attitude problems. Injury involving lost time in the workplace	Widespread staff issues cause failure to deliver several minor strategic objectives	Staff issues cause widespread failure to deliver essential services. Temporary disability or hospital admission < 3 days	Death or permanent disability or long term hospital admissions
	Environmental	Minor adverse event that can be remedied immediately	Isolated instances of environmental damage requiring effort to fix in the short term	Adverse events that cause widespread damage but reversible in the short to medium term. May incur cautionary notice or infringement notice	Significant adverse event causing widespread damage which may be reversed through appropriate remedial action in the medium term. Penalties may apply	Major adverse event requiring continual long term remedial action. Significant penalties may apply
	Financial	Financial impact (expenditure or revenue) <$50,000 Budget variation manageable in the short term	Financial impact (expenditure or revenue) between $50,000-$250,000 Budget variation manageable without impact on bottom line of budget absorbed over current financial year.	Financial impact (expenditure or revenue) between $250,000 - $500,000 Impact on budget beyond current financial year but manageable within next financial year	Financial impact (expenditure or revenue) between $500,000 - $1million Impact on budget with recovery over proceeding two or three financial years	Financial impact (expenditure or revenue) >$1 million on budget with recovery over three or more financial years
	Service delivery/ IT	Interruption to a service not requiring any further remedial action and with minimal impact on customers	Interruption to a service requiring further remedial action and with moderate impact on customers	Interruption to core business function or essential service with significant customer impact for up to 48 hours	Interruption to core business function or essential service for 2-7 days	Interruption to core business function or essential service greater than 7 days
	Infrastructure & Assets	Some damage where repairs are required however facility or infrastructure is still operational	Short term loss or damage where repairs required to allow the infrastructure to remain operational using existing internal resources	Short to medium term loss of key assets and infrastructure where repairs required to allow the infrastructure to remain operational. Cost outside of budget allocation	Widespread, short term to medium term loss of key assets and infrastructure. Where repairs required to allow the infrastructure to remain operational. Cost significant and outside of budget allocation	Widespread, long term loss of substantial key assets and infrastructure. Where infrastructure requires total rebuild or replacement.
	Legal/ Compliance	Dispute resolved through internal process or expertise	Dispute resolved through legal advice	Corporation directed to undertake specific activities to remedy breaches in legislation that may require the involvement of legal firms	Deliberate breach or gross negligence/formal investigations from third party (Ministerial involvement, Ombudsman or QCCC)	Major breach of legislation resulting in major corporation penalties, fines, QCCC investigation that may result in legal action against corporation staff or class action
	Political/ Reputational	Political activity that requires minor changes in operations Issue may result in a number of adverse local complaints	Political activity that requires changes in operations Issues may attract limited media coverage	Political activity that requires changes in operations with budget and resource implications Issue may attract regional and state media coverage through various mediums with minimal consequence	Political activity that requires changes in operations with significant ongoing budget or resource implications Issue may attract significant State and National media coverage with some effect on Councils reputation	Political activity that results in irreparable damage Prolonged adverse media attention. Staff and Elected members forced to resign.

Risk Rating Matrix

Inherent risk is the overall raw risk. It is determined by combining the likelihood and the consequence rating. The level of inherent risk will determine how each risk is treated. The following matrix shows the inherent risk levels that will be used by Council.

		Consequence				
Likelihood		Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Almost Certain	5	6 Moderate	7 Significant	8 Extreme	9 Extreme	10 Extreme
Likely	4	5 Moderate	6 Moderate	7 Significant	8 Extreme	9 Extreme
Possible	3	4 Low	5 Moderate	6 Moderate	7 Significant	8 Extreme
Unlikely	2	3 Low	4 Low	5 Moderate	6 Moderate	7 Significant
Rare	1	2 Low	3 Low	4 Low	5 Moderate	6 Moderate

Risk Rating Matrix

4.3 RISK EVALUATION

Risk evaluation is about deciding whether risks are acceptable or unacceptable. The term "as low as reasonably practicable" (ALARP) will be used where risks are assessed, evaluated and determined to be acceptable.

For a risk to be ALARP it must be possible for the risk owner to demonstrate that the cost involved in reducing the risk further would be grossly disproportionate to the benefit gained. The ALARP principle arises from the fact that infinite time, effort and money could be spent on the attempt of reducing a risk to zero with little or no further benefit to Council or the community.

The purpose of risk evaluation is to assist in making decisions on the outcomes of the risk analysis; in particular which risks require further treatment and the priority for implementing those treatments.

Where risk treatment produces a business benefit, further control is necessary, and a risk treatment plan will need to be developed.

Generally, risks with extreme and significant risk ratings will require further treatment. Risks with low and moderate risk ratings need to be considered together with the context to determine if further treatment is necessary. Risk evaluation involves comparing the level of risk (Risk Rating) against Council's known priorities and requirements. The treatment strategy for each risk will vary depending on the determined level of inherent risk.

Extreme - requires immediate action as the potential risk exposure could be devastating. Action may include detailed research, planning and decision making at the Senior Management Level.

Significant - requires action very soon as it has the potential to be damaging to the organisation. Senior Management attention an action needed.

Moderate - requires treatment with routine or specific procedures. Management responsibility must be specified.

Low - continue to monitor and re-evaluate the risk, ideally treat with routine procedures.

Risks that affect other Council departments/sections/units need to be communicated to those areas and in-turn those people need to be included in the analysis and evaluation processes to ensure that risk treatments are appropriate from a whole of Council perspective.

Any risks where the calculation is thought to be too high or too low are to be adjusted and documented accordingly. The output of the risk evaluation is a prioritised list of risks requiring further action. Low or acceptable risks should be monitored and periodically reviewed to ensure that they remain acceptable.

Risks ranked as **Moderate and Low** are to be reviewed by the person with the delegated operational responsibility on an annual basis. The outcome of the review and any changes to the risk exposure are to be reported to the relevant Director. No treatment plans required for risks identified at this level.

Risks ranked as **Extreme and Significant** require detailed analysis of practices and controls to determine the residual risk rating. Risks with an inherent risk of extreme or significant will be actively managed by the CEO who will determine any delegation of the process. A treatment plan will be developed where appropriate to improve the residual risk. The CEO will report to Council on the status of these risks, with the worsening of any extreme risks being reported to the Mayor immediately. Any other significant change to Councils risk exposure will be reported to the Council as soon as possible.

Councillors acknowledge that it is not appropriate or in the best interest to stakeholders, to eliminate all risks. A component of risk evaluation is also to consider if the current control measures are sufficient and that the risk is appropriately managed.

Further Classification of Risks
Risks may be classified even further into the following zones:

Generally Acceptable (GA): in the area of the chart ranked "low", risks have little impact and or are unlikely to occur. Risks in this region don’t pose an immediate threat to the project or organisation, and some can even be ignored.

As Low As Reasonably Possible (ALARP): This is a zone of acceptable risk including "low" and "moderate" ranking areas. Risks within this region of the matrix are tolerable or not significantly damaging; work can proceed without addressing the risks immediately.

Generally Unacceptable (GU): this is the area of the chart where risk is "Significant" or "Extreme". Risks in this region are quite damaging, highly likely to occur and would threaten the project or organisation. They are highest priority and must be addressed immediately.

5. TREAT THE RISKS

Risk treatment involves identifying the range of options for treating unacceptable risks, assessing the options, preparing risk treatment plans and implementing them.

Risk treatment involves a cyclical process of:

- Assessing a risk treatment;
- Deciding whether residual risk levels are tolerable;
- If not tolerable, generating a new risk treatment; and
- Assessing the effectiveness of the new treatment.

Treatment options include;

1 Preventative - These types of controls focus on preventing the risk occurring.
2 Detective - Detect risk or issues and report.
3 Corrective - These controls typically respond, recovery, and prevent further occurrences.
4 Recovery-focused - This control is not a matter or reducing the risk but a reduction in the consequence by having efficient processes for recovery.
5 Directive - Direct adjustment in policies, procedures or guidelines.

Deterrent - Introducing an element that discourages violations or the risk
Treatment plans should clearly identify the priority order in which the individual treatments should be implemented. Where a number of treatments are available, a tool to determining the best option (or most viable option) is a cost benefit analysis. Where a risk is 'extreme' the executive management team and the audit committee may approve a specific risk treatment plan to manage the risk.

6. MONITOR AND REVIEW OF RISKS

The risk register will be reviewed and updated on an annual basis, or more frequently where a new or changed risk is identified in the Council reporting process. Once changes have been reviewed and agreed upon by the appropriate members of the Senior Management Team, the Audit Committee should review the risk registers, as presented, for adoption by Council.

Monitoring and review ensures that changing context and priorities are managed and emerging risk are identified. Included in this step are:

- Monitoring and review of controls (effectiveness, adequacy, changes in risk environment etc);
- Learning lessons from successes and failures in terms of root causes and control effectiveness;
- Improving the risk management process; and
- A combination of audit processes and line management review etc.

All risk assessments and treatments will be conducted in accordance with the ERM Process. All relevant documentation must be placed in Council’s electronic recordkeeping system. The Manager Development & Governance will collate all risks into the Risk Register for future monitoring.

Risk reports should be presented to Council through the Audit Committee where possible. The Manager Development and Governance will report at least annually on:

- Significant and Extreme risks; and
- Any risks that have been identified as requiring treatment; and
- Full details of any risks previously adopted by Council or new risks that have been added or amended since previous report;
- All risks assessed as being ALARP (tolerable).

Council must provide direction as to their continued acceptance of specific risks and agreed controls or treatments.

7. RECORDING AND REPORTING

Recording is an integral part of Council's governance and seeks to:

- Disseminate risk management activities and outcomes across Council;
- Provide information for decision-making;
- Improve future risk management activities;
- Assist interaction with all relevant stakeholders.

Factors for inclusion in the reporting activities include:

- Specific stakeholder information needs;
- Cost, frequency and timeliness of reporting;
- Method of reporting;
- Relevance of information to Council's objectives and decision-making.

Decisions on the creation, retention and storage of documented information should be made in accordance with Council's Records Management Policy.